2

CDRL #004

SPARTA, INC.

DDN Trusted Guard Gateway

AD-A196 891

Trusted Guard Gateway (TGG) Requirements Analysis and Detailed Description

May 10, 1988

Contract No. DCA100-87-C-0095

Prepared For:

Defense Communications Engineering Center
Defense Communications Agency
Code R640, ATTN: COR
1860 Wiehle Avenue
Reston, VA 22090-5500

DTIC
ELECTE
JUN 03 1988
D

SPARTA, Inc.
7926 Jones Branch Drive
Suite 1070
McLean, VA 22102
(703) 448-0210

document has been approved
release and sale; its
is unlimited.

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188
Exp Date Jun 30 1986

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS N/A
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT UNLIMITED
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION SPARTA, INC. 6b OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION DEFENSE COMMUNICATIONS ENGINEERING CENTER
6c. ADDRESS (City, State, and ZIP Code) 7926 JONES BRANCH DRIVE SUITE 1070 MCLEAN, VIRGINIA 22102	7b. ADDRESS (City, State, and ZIP Code) 1860 WIEHLE AVENUE RESTON, VIRGINIA 22090
8a. NAME OF FUNDING/SPONSORING ORGANIZATION DCEC 8b OFFICE SYMBOL (If applicable) R640	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER DCA100-87-C-0095
8c. ADDRESS (City, State, and ZIP Code) 1860 WIEHLE AVENUE RESTON, VIRGINIA 22090	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11. TITLE (Include Security Classification)
TRUSTED GUARD GATEWAY (TGG) REQUIREMENTS ANALYSIS & DETAILED DESCRIPTION

12. PERSONAL AUTHOR(S)
SPARTA, INC.

13a. TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
FINAL	FROM 6/10/87 TO 5/10/88	880510	68

16. SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	COMPUTER NETWORKS, DEFENSE DATA NETWORK, INTERNETWORKING, GATEWAY

19 ABSTRACT (Continue on reverse if necessary and identify by block

This document provides to the Defense Communications Agency (DCA) the results of a user requirements collection and analysis effort made for the purpose of determining the need for a specialized gateway that would interconnect communities with different security characteristics (such as allowing multilevel secure, classified hosts operating at the unclassified level to communicate with hosts in the unclassified segment). Section 2 of this report discusses the evolution of the DDN with regards to interoperability abd security. Section 3 reviews the results of a survey of DDN subscriber requirements describing the survey method and postulating the numbers and types of gateways required. Section 4 is an analysis of the potential functions to be performed. Section 5 presents a survey of current commercial & government gateway technology. Section 6 presents an analysis of the numbers of TGG required for the DDN.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL MR. J. STEVE LLOYD	22b TELEPHONE (Include Area Code) (703)437-2175 22c OFFICE SYMBOL R640

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

EXECUTIVE SUMMARY

The purpose of this report is to provide to the Defense Communications Agency (DCA) the results of a user requirements collection and analysis effort made for the purpose of determining the need for a Trusted Guard Gateway (TGG) that would interconnect communities with different security characteristics (such as allowing multilevel secure, classified hosts operating at the unclassified level to communicate with hosts in the unclassified segment). This effort surveyed users to substantiate the operational need for such a gateway, define its specific functions, and assess the numbers needed.

The user survey indicated a clear need for communication services between Defense Data Network (DDN) segments. While the plans, requirements, and designs for many of the systems contacted were still in a preliminary or tentative state with respect to the DDN, current operational needs and projected evolutionary paths indicate a requirement for a TGG. Not only are the TGG services needed, but concern and desire for a more specialized upgrading and downgrading service was expressed. The survey indicated that intersegment communication services will be an essential part of the DDN transition to the DISNET/MILNET environment.

Based on user requirements and DDN network and security architectures, this report defines functional, assurance, and performance requirements for a single TGG needed to support the range of operational and security needs. The survey of user mission requirements has indicated some potential conflicts with current policy as expressed in the security architecture. One example is the prohibition on intersegment virtual terminal service. The TGG requirements definition does not arbitrate the policy for a given operational scenario (e.g., ARPANET/MILNET or MILNET/DISNET), but rather defines a tool to support and enforce the policies established by DoD.

This report establishes the requirements for a TGG and has identified an approach that can meet user requirements in a secure fashion. An examination of gateway technology indicates a number of potential bases for TGG implementation. COMPUSEC certification is likely to be the largest challenge in the TGG development and acquisition. Addressing these issues will be an important part of the next phase of the Trusted Guard Gateway effort.

1.0 Introduction

The purpose of this report is to provide to the Defense Communications Agency (DCA) the results of a user requirements collection and analysis effort made for the purpose of determining the need for a Trusted Guard Gateway (TGG) that would interconnect communities with different security characteristics (such as allowing multilevel secure, classified hosts operating at the unclassified level to communicate with hosts in the unclassified segment). This effort surveyed users to substantiate the operational need for such a gateway, define its specific functions, and assess the numbers needed.

Section 2 of this report discusses the evolution of DDN with regard to interoperability and security. The Defense Data Network (DDN) security architecture identifies distinct segments that serve particular operational elements: DISNET for classified subscribers; MILNET for unclassified operational subscribers; and ARPANET for the research community and the world at large (through the Internet). DCA, in concert with NSA, has addressed the need for communication between these segments subject to appropriate controls. In order to maintain appropriate security throughout the DDN, and in order to provide consistent levels of assurance within communities, gateways interconnecting these segments must provide certified access control and labeling functions.

Section 3 reviews the results of a survey of DDN subscriber requirements describing the survey method and postulating the type of gateway required based on conclusions drawn from the survey. Extensive use of the User Requirements Data Base (URDB) along with interviews with network planners and users provided substantial feedback. This survey identified user communities with a clear need for service between DDN segments, particularly between MILNET and DISNET. The support of database and MIS systems spanning these segments will require a TGG. The nature of these applications necessitates the flexibility in access control described in Section 4.

Section 4 is an analysis of the modes of operation for a TGG and an examination of the functions to be performed. An IP gateway, a transport protocol relay, and an application relay were examined as TGG architectural alternatives. An augmented IP gateway was selected as the most viable option in terms of complexity, performance, and functionality. The TGG must provide certified security services including labeling, access control, and flow restriction as well as fit into an overall monitoring, control and audit structure. The choice was made to define a flexible TGG capable of operating in multiple scenarios and evolving along with the overall DDN policies and security posture. Specific capabilities include labeling datagrams as untrusted

by means of the IP security options, performing access control based on IP addresses and TCP port IDs (i.e., using TCP port IDs to determine the application), and limiting flows based on varying thresholds. This section considers additional security requirements that must be provided for dual-homed hosts. A host homed on multiple segments can act as a *de facto* TGG. In order for the security provided by TGGs to be effective, all paths between segments must be secured. The requirements for multi-homed hosts must be augmented to take into account the fact that such entities are general purpose systems supporting a full range of user activities. To provide security a multi-homed host must limit the degree to which users accessing it via an untrusted network can run processes or otherwise control its resources.

Section 5 presents a survey of current commercial and government gateway technology. These technologies are assessed in terms of hardware and software functionality, performance, and certification possibilities for a TGG. Any gateway product used as a base for the TGG would require modifications and enhancements in light of the new and unique requirements. While many products offer promise with respect to functionality and performance, certification and certifiability are a major concern. Experience to date has shown that certification is a major program obstacle in terms of cost, schedule, and risk. Consequently, further examination of paths for implementation should pay particular attention to hardware bases with certified operating systems in place.

Section 6 presents an analysis of the estimated number of TGGs required for the DDN. This section concentrates on TGGs required to support the MILNET/DISNET interface. The assumptions driving the calculation of the estimates are provided as is a discussion of obstacles associated with deriving estimates for each TGG scenario.

2.0 Trusted Guard Gateway Concept

In the 1989 time frame and beyond, the DDN will require Trusted Guard Gateways (TGGs) to securely allow limited, controlled communications between segments of the DDN operating at different levels of trust or at different security levels. TGGs have been described in DCA plans for the growth and evolution of the DDN.[1 2 3] This section describes the planned role of TGGs in the DDN. Section 2.1 reviews the TGG roles described in "DDN Evolution of Security Services"[2]. Section 2.2 discusses the specific types of TGGs and their roles among DDN segments. Section 2.3 examines the TGG generic role in providing interoperability while maintaining security services.

2.1 DDN Evolution and Security Architecture

The DDN evolution is greatly affected by the diverse security and operational requirements of network subscribers. The DDN security architecture evolution has addressed specific needs of classified subscriber communities while maintaining economic approaches to network development and operation. Currently, the DDN consists of multiple physically distinct segments based upon these differing subscriber needs. ARPANET supports continuing access to research and development activities and access by a very wide scientific and academic community. MILNET supports unclassified operational needs of DoD agencies. The needs of classified subscribers segregate more naturally into communities of interest. DISNET will be the major integrated network segment serving classified subscribers. WINCS and SCINET serve the WWMCCS and SCI communities respectively.

The DDN Security Services Evolution document[2] addresses six types of security services, how they are supported for unclassified subscribers and for classified subscribers, and the security evolution of DDN elements (including policies, procedures and architectural elements). The six security services are:

1. Data confidentiality: mechanisms to prevent unauthorized disclosure of data;
2. Data integrity: mechanisms to prevent unauthorized modification of data;

---

1 DCA, "DDN Master Engineering Plan"

2 DCA, "DDN Evolution of Security Services, 1986 - 1992"

3 DCA, "DDN Subscriber Guide to Security Services, 1986-1992"

3. Identification, Authentication and Access Control;
4. Data origin authentication;
5. Non-repudiation: mechanisms to certify to the sender that data were received;
6. Availability: mechanisms to support assured service of DDN and subscriber resources.

The DDN Security Services Evolution document presents the TGG as:

- a support for data confidentiality for both classified (p. 21) and unclassified subscribers (p. 13)
- a support for identification, authentication and access control for both unclassified (p. 17) and classified (p. 25) subscribers
- a support for data origin authentication services for classified subscribers (p. 27).

The document describes the TGG as providing interoperability between communities of different security levels (p. 53), different trust levels (p. 39) and between open and closed communities. It does not envision a TGG role in non-repudiation or in data integrity. While a TGG role in availability is not explicitly discussed, Sections 2.3 and 4.4 outline TGG relevance for assuring service.

The DDN Security Services Evolution states that DCA's plans are to provide for both security and interoperability among DDN segments and between open and closed DDN communities. This report on user requirements and detailed technical descriptions of the TGG supports the execution of these plans.

The evolution of the DDN architecture has taken place in concert with NSA. The INFOSEC organization of NSA has contributed and reviewed architecture material to support the provision of comprehensive security. The NSA activities have included the development of security systems for individual DDN segments (e.g., BLACKER for DISNET) and the definition, review, and approval of requirements for security across all segments. These requirements have specified mechanisms and levels of trust appropriate for network elements, for hosts, and for the interconnection of segments.[4]

Interconnection requirements define functions and assurance levels such that connection to a less secure segment does not compromise the security of the more secure segment. These requirements are addressed in

---

4 NSA: "INFOSEC Review of the DDN Security Architecture", CSC-TR-26-86, 4 APR 86

detail for both ARPANET/MILNET and MILNET/DISNET scenarios and directly apply to TGG operation. These requirements dictate the restriction of applications (mail and file transfer), the prevention of flooding, the labeling of data, and suggest appropriate assurance levels (B2 for MILNET/DISNET and B1 for ARPANET/MILNET). These requirements serve as a basis for TGG security requirements. Actual requirements reflect a balance between these statements and the operational needs determined in the user survey. The resulting compromise must be evaluated for the security provided in the overall DDN.

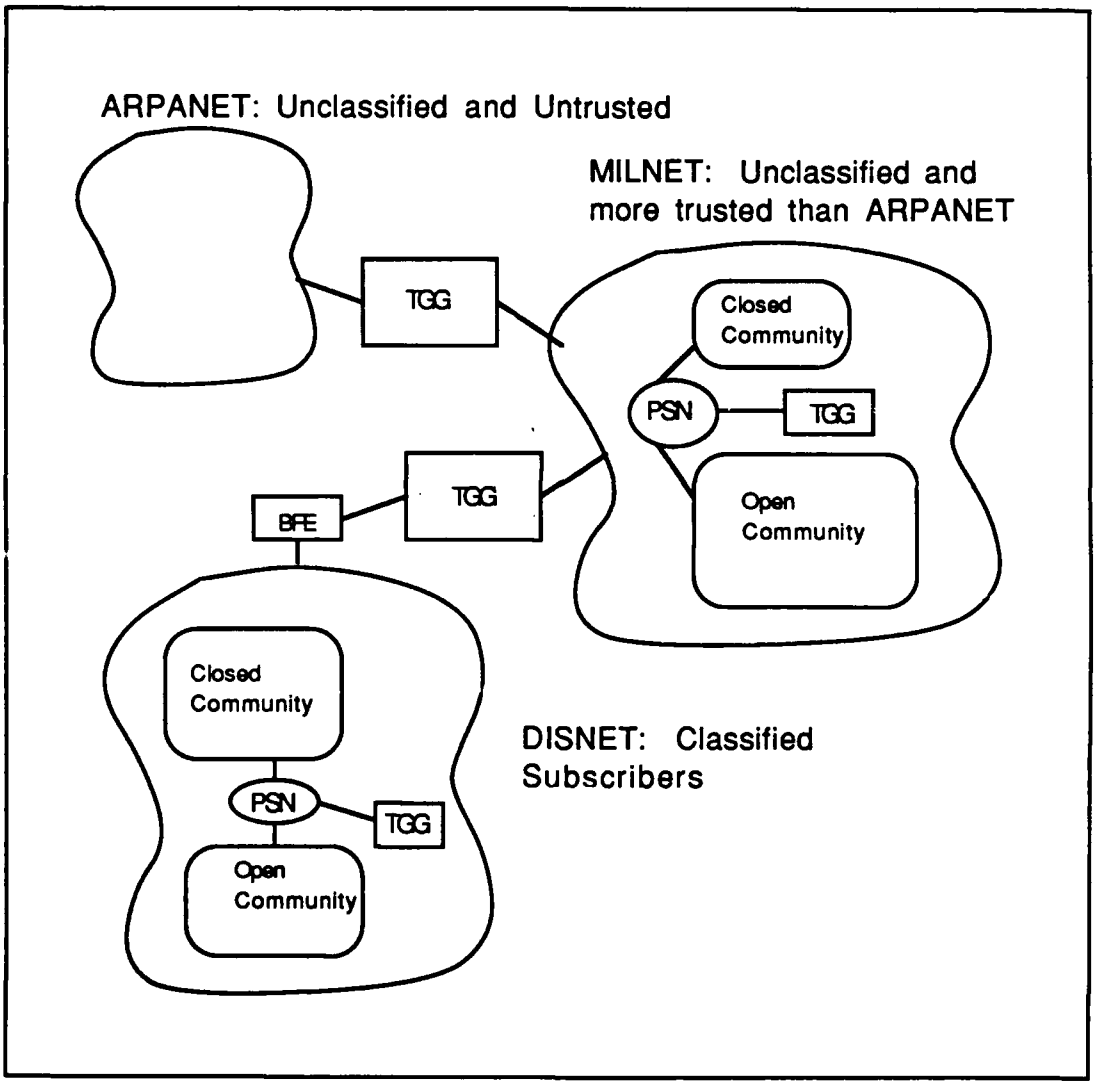


Figure 2.2-1 TGG Roles Among DDN Segments

2.2 Candidate TGG Scenarios

DCA plans for the TGGs to support limited interoperability among the MILNET, DISNET and ARPANET. In addition, the TGG must support interoperability between communities operating at different trust levels within MILNET or DISNET. In this last case, packet switches enforce non-interoperation between the communities; TGGs allow limited, discretionary interoperation. Figures 2.2-1 and 2.2-2 illustrate the relationship between the three major DDN segments, related levels of trust, and information flows through TGGs.

DCA has defined[5] traffic control capabilities of TGGs based upon the application-level protocols that are exchanging data between hosts. For example, current ARPANET/MILNET gateways support the exchange of electronic mail messages. The TGG interoperation requirements with respect to DoD application layer protocols are as follows:

- Two-way electronic mail message exchange via SMTP is permitted.
- File transfers are permitted only if initiated by a host within the high side network. Files may be transferred in either direction under the control of the high side host.

Two major traffic control capabilities are required of TGGs:

- The TGG shall mark all data moving from the low side network to the high side network. The marking will reflect the level of source authenticity and trust.
- The TGG shall be capable of limiting the rate at which datagrams are relayed from the low side to the high side network as well as the rate at which designated events take place.

The following sub-sections identify TGG scenarios to support interoperability among and within DDN segments. These types include (1) a MILNET/DISNET TGG, (2) an ARPANET/MILNET TGG, and (3) a Closed/Open Community TGG.

---

5 DCA, "Statement of Work. Trusted/Guard Gateway Development. SOW R640-87-415"

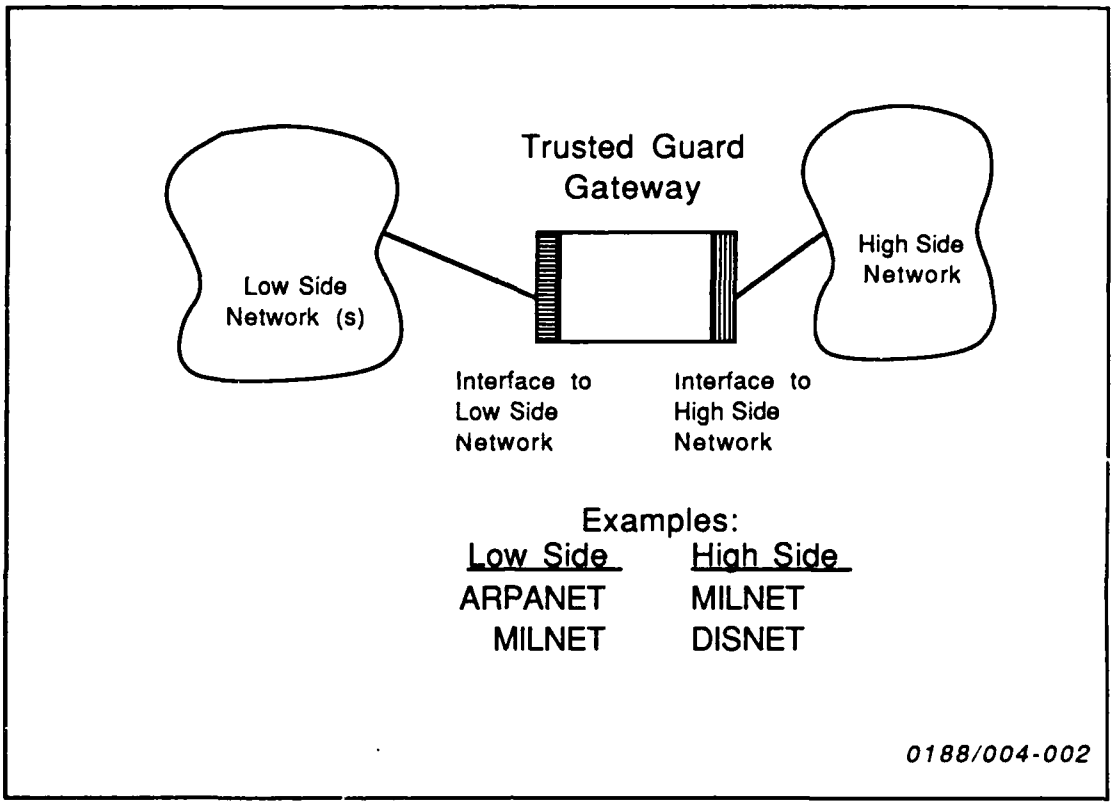


Figure 2.2-2 TGG Schematic

2.2.1 The MILNET/DISNET Trusted Guard Gateway

The MILNET/DISNET TGG would support communications at the unclassified level between hosts on the MILNET and attached networks (the low side) and hosts on the DISNET and attached networks (the high side.) Two modes of operation have been considered for this gateway: (1) to operate at the unclassified level only to support unclassified communications between the high and low sides, and (2) to operate at the unclassified level on the low side, but at a higher sensitivity level on the high side. In this latter case, the TGG upgrades data going from the low to the high side, and downgrades data in the opposite direction.

At this time, providing a general purpose service between classified and unclassified hosts that is capable of securely downgrading data is beyond the state of the art. The context sensitive nature of such services requires application-specific downgraders (see section 4.4). The TGG relies on the BLACKER system on the DISNET to enforce mandatory access control and to prevent any classified datagrams from reaching the TGG.

2.2.2 ARPANET/MILNET Trusted Guard Gateway

Communications between ARPANET and MILNET have remained at a significant volume since the ARPANET/MILNET split in 1983. These exchanges will remain necessary in order to support the interaction between defense and non-defense research and technology activities. DoD subscribers must access non-DoD resources and data and need to selectively make information externally available. Mail Bridge gateways currently carry this traffic and are heavily loaded. They provide some degree of limitation of access to MILNET by ARPANET hosts, but they can be circumvented.

ARPANET/MILNET TGGs will replace existing mail bridges and other gateways between ARPANET and MILNET. They will be capable of permitting electronic mail transfers between ARPANET and MILNET while limiting other traffic.

2.2.3 Closed/Open Community Trusted Guard Gateway

A major component of the DDN Security Services Evolution is the certification of subscriber hosts within MILNET and DISNET to the C2 level or better. This will provide increased confidence in a host's ability to provide the protection of resources and data.

However, not all hosts will achieve C2 certification, and some will achieve this status sooner than others. In order to provide continuing protection for certified hosts, non-certified hosts will be placed into Closed communities. Closed communities may interoperate among themselves but will be prevented from interoperation with certified hosts in the Open community. Packet switches will enforce the segregation.

DCA anticipates that some interoperation will be necessary between Closed and Open communities. The Closed/Open Community TGG will provide a means for limited communications between the Open and Closed communities. Hosts from these two types of communities can communicate, when authorized, using the Internet Protocol via the Closed/Open Community TGG. The Closed/Open Community TGG identifies two classes of network addresses rather than two network interfaces as its high and low sides. It performs TGG services based upon these addresses including marking data, access control, and flow control.

2.2.4 Additional TGG Scenarios

Several scenarios have been discussed in which the TGG would be able to provide services in the DDN. These scenarios have involved the separation of communities with a clear need to interoperate, yet which operate with different security attributes. In order to maintain the security properties of these communities it is necessary to restrict the flow and type of

information crossing the boundaries. To date, three applications of this service have been defined: a gateway between the ARPANET and the MILNET; between the MILNET and the DISNET; and between Closed and Open communities in the MILNET or DISNET.

The set of functions defined for the TGG in this document allow for a potentially wider application of TGGs. Such an expanded role has a number of advantages in terms of the development and procurement of a TGG. A wider application increases the importance of a TGG and potentially reduces the unit cost. A number of additional candidate scenarios have been identified. The first scenario is as a gateway between the DISNET and LANs or other subscriber networks directly connected to the DISNET. This gateway could provide enhanced control and protection for both sides of the interface. The second is a gateway between US and Allied networks, particularly in theater environments. Such a gateway could provide both access control and security functions as well as supporting interoperability. A third scenario is to provide support for Department of State requirements where their networks or subscribers use the DDN as a backbone. While such a scenario is not currently planned, it could represent an extension of the current plans for the Department of State Telecommunications Network (DOSTN). Each of these scenarios has characteristics in common with the applications already defined and represents a natural extension of TGG use.

The concept for the DDN is evolving from one of a common communication service for DoD hosts to a common communication backbone for a wide range of DoD subscriber networks. The ARPANET is already 80% gateways and the other DDN segments are expected to move in the same direction. The networks that connect to the DDN in this way will span a large range of security levels, sizes, certification statuses, applications, and interoperation requirements. The assortment of equipment that may comprise these subscriber systems and the gateways that will connect them may perform in a variety of ways. Due to this diversity, it may be desirable to both protect the DDN from subscriber systems and to protect subscriber systems from other subscribers. A TGG at the interface to the DDN could also be used by administrators of subscriber systems to control the capabilities of their own users. This dichotomy obscures the definition of high side and low side which is clear in the three well-defined scenarios for the TGG. This dual role may result in a TGG which enforces its restrictions equally in both directions (this should simply be part of the configuration of a normal TGG).

Possible connections may also exist between US networks and Allied communication systems, especially in theater environments such as Europe or the Pacific. These environments require close cooperation and communication, particularly at the tactical level during engagements or exercises, as well as in anticipation and in support of such activities. Such

operation may be characterized by limited applications, differing security classification systems and interpretations, differing security systems, and differing rules for interconnection, and possibly differing network technologies. The lack of a hierarchical relationship between the parties involved also complicates the situation. For these types of application there is no high or low side or any other ordering. In order to accommodate the administrative and control needs of such interfaces, two TGGs may be required, one operated by each side of the connection. The presence of one or more TGGs at these locations could provide a convenient place to interconnect differing security and networking technology domains.

2.3 TGG Concept Summary

The wide range of interoperability that is possible within the DDN poses both opportunities and risks for subscribers. To manage the security risks associated with interoperability, DDN subscriber security services are provided as a part of the DDN architecture. The aim of the TGG is to provide interoperability within that architecture while maintaining and supporting the security services of the DDN.

The risks to subscriber data and resources result from the way in which computers provide access to them. Users have accounts on hosts that permit them to establish sessions (i.e., "log in"), edit text files, compile source code to produce executable objects, access files and databases, and initiate the execution of system utilities and user-written programs. To date, there are relatively few single-host operating systems that securely control these activities in accordance with mandatory or discretionary access control policies. The recourse in many cases is to operate such systems in physically secure environments for approved, cleared users only.

Internetworking provides the means for remote users to log on to systems connected into the DoD Internet. The DoD Internet protocol[6], IP, furnishes an address space that spans multiple networks. This approach has been effective in promoting wide interoperability. Current gateway designs treat IP datagrams independently with little regard for the origin. The destination indicated by an IP datagram is used for routing decisions. IP gateways provide limited packet switching services with little error recovery and no tracking of packets for possible retransmission. In practice, this design makes congestion control difficult because there is no concept of streams of data. Consequently, an offending stream source cannot be easily identified for the exercise of flow control messages.

---

6 MIL-STD-1777, "Military Standard Internet Protocol," 12 AUG 83

In the current DoD Internet architecture, remote users access a host's resources via higher level protocols that use the unreliable network services of IP and gateways. A reliable transport service is provided by MIL-STD TCP[7], which uses IP directly and performs value-added services at the source and destination. Application level protocols, including TELNET[8], FTP[9] and SMTP[10], use TCP for reliable, sequenced data exchanges. TELNET and FTP operate under direct user control while SMTP operates under indirect user control. In contrast, TCP and IP are rarely under direct user control, although this is possible. In other words, the Internetwork permits long-range user access to hosts, using services built upon the Internetwork Protocol, IP.

A marked growth in the number and types of local area networks (LANs), particularly those being developed by the individual military departments (MILDEPs), is forcing the issues of security, network management, and gateway development to the forefront of internetworking problems.[11] Responsibility for gateway development and management is assigned to the individual MILDEPs yet their focus is on selecting LANs specifically designed to solve a localized communication problem (e.g., interconnecting systems on a military base). While the selection of LANs is generally motivated by the functions and performance required by local users, gateways are essential in providing interoperability. LANs support interoperability with users across the DDN by means of the standard data exchange protocols: IP, TCP, TELNET, FTP and SMTP.

The functions performed by TELNET, FTP, and SMTP motivate consideration of the access control to be performed by the TGG. While their use can pose threats to user data, the threats can be mitigated by the access control performed by the TGG as follows:

- TELNET provides an Internet equivalent of a dial-up line to a host. When a TELNET connection is made, the remote user has the privileges and access capabilities usually accorded to a directly connected user. For this reason, TELNET connections between hosts in environments of different trust levels are not permitted.

---

7 MIL-STD-1778, "Military Standard Transmission Control Protocol," 12 AUG 83

8 MIL-STD 1782, "Military Standard TELNET (Virtual Terminal) Protocol," 10 MAY 84

9 MIL-STD 1780, "Military Standard File Transfer Protocol," 10 MAY 84

10 MIL-STD 1781, "Military Standard Simple Mail Transfer Protocol," 10 MAY 84

11 DDN Premises Technology Study, BBN, 1986

- FTP enables transfer of files between hosts under interactive user control. Files may be ASCII or binary. The transfer of executable files and the ability to browse through remote file systems are of particular concern. This concern focuses on FTP initiated from a low side environment that connects to a high side environment.
- SMTP supports the transfer of queued text messages between systems, with or without interactive user control. SMTP's limitations along with its utility recommend that it be allowed as a general means of interoperability between environments.

These considerations, together with the current DDN security architecture that separates users into segments, provide the motivation for an access control, or Guard, gateway capable of selectively passing datagrams among these segments as a means of permitting interoperability. Such a gateway is a necessary part of the DDN architecture and this report provides a justification and a rational basis for planning for the acquisition of TGGs for the DDN. This report identifies user requirements in order to provide a quantitative estimate of the numbers of TGGs, and provides detailed technical descriptions of TGGs within the DDN network and protocol architectures.

While three or more scenarios have been identified above in which a TGG might operate, the commonality in function and role argue for a single TGG. A single technical design for a TGG will be sufficient for the three inter-segment requirements outlined above. TGGs will be capable of enforcing a variety of policies determined by the administration rather than establishing a policy by design. The different scenarios will therefore be characterized by a change in configuration rather than by a change in hardware.

The TGG in all cases will be able to perform data labeling for all upward bound data and will enforce access controls over such data in accordance with host-pair or application protocol based policy. Further access control policy definitions are needed for all three TGG scenarios. Additionally, host-pair access control methods are needed for all three scenarios and must be implemented in an easy-to-use fashion.

3.0 User Requirements Survey

This section reports the results of surveying major DDN subscriber communities with regard to the need for and utility of TGGs. The aims of the survey were to validate subscriber TGG requirements and to identify the numbers and types of TGGs required.

Presented in Section 3.1 are the methods employed and results obtained during the survey. The priorities afforded to the types of TGGs can be found in Section 3.2. Section 3.3 presents conclusions regarding the user survey and the usefulness of the User Requirements Data Base (URDB) as a planning and tracking tool for the evolving DDN. Finally, subjecting the assessment of the survey results to calculations based on known gateway functionalities and requirements, an estimate of the number of MILNET/DISNET TGGs required was developed. The reader is referred to Section 6.0 for this estimate.

3.1 User Requirement Review Methods and Results

The survey of DDN user requirements utilized two primary sources: (1) the User Requirements Data Base (URDB), and (2) interviews with selected planners within the DoD community. This section documents the process of gathering and synthesizing data from these sources.

A major goal of the survey was to gather information focused specifically on subscribers whose applications would require the services of a TGG. Interviews with high-level planners helped to provide valuable insights, but only indirectly identified application communities. Ultimately, identifying these specific application communities became one of the most elusive tasks of the survey. Initial queries to the URDB attempted to identify major DDN subscribers requiring connectivity across more than one DDN segment.

3.1.1 URDB Consultation

The URDB is the information repository for subscribers' validated requirements for DDN network connectivity, and it contains descriptions of subscriber hosts and terminals and intended sources and destinations for data communications. Data is organized into a collection of relational data bases. The objective of consultations with the URDB was to identify users and systems who will definitely require or who can potentially benefit from TGGs. Our survey began with a study of the definitions of these relational database files[12].

---

12 "Defense Data Network Management Information System (DDN-MIS) Data Base Specification (Update), 27 February 1987, Prepared for DCA Code B622 by GTE, Report. No. 00-2479541.

The URDB specification describes data base files in terms of fields. Based upon our review of the specification that provides detailed definitions of each field, the files listed below were found to be of interest. Read-only access to them was requested and granted by the URDB administrator.

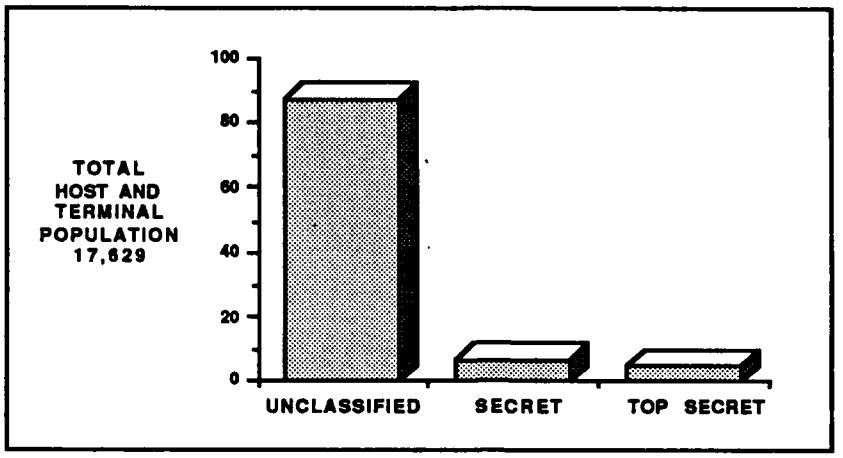
1. DDN-SEC-CLASS-CODES contains the set of security classification codes used in other files. A single letter code and its expansion to 10 letter and 40 letter fields are included.
2. DDN-AGENCY-CODES contains the set of subscribers' agency names and associated two letter codes.
3. DDN-CONNECTION2 contains a separate record for each terminal or host connected to the DDN. System parameters including interface codes, line speeds, security levels, net address and assignment, IMP port assignment, system acronym, technical point-of-contact name, address and telephone data are also included.
4. DDN-HOST2 contains a separate record for each host connected to the DDN. Data includes security certification code, name of location of major military command, and the name, address and telephone for the host administration point of contact.
5. DDN-SYSTEM-NARRATIVE contains narrative information record for each major DDN system.
6. DDN-SYSTEM-MASTER2 contains a record of basic information about each major DDN system, including the system full name, agency, assigned net, numbers of proposed hosts and terminals, and the name, address and telephone of the system point of contact.
7. DDN-TRAFFIC-MATRIX2 contains a record for each host-to-host or terminal-to-host connection. URDB numbers for the destination and originators are also included. The estimated traffic is furnished via transmission unit and rate. Each record contains the acronym identifier for its associated DDN major system.

3.1.1.1 Preliminary Statistics Gathering

Employing the HISTOGRAM function, available in the ADABAS NATURAL language, in conjunction with the DDN CONNECTION2 file, numbers of hosts and terminals at particular classification levels were

gathered. Table 3-1 illustrates the percentages at each classification level over a total DDN host and terminal population.

TABLE 3-1 CLASSIFICATION LEVELS OF DDN HOSTS AND TERMINALS



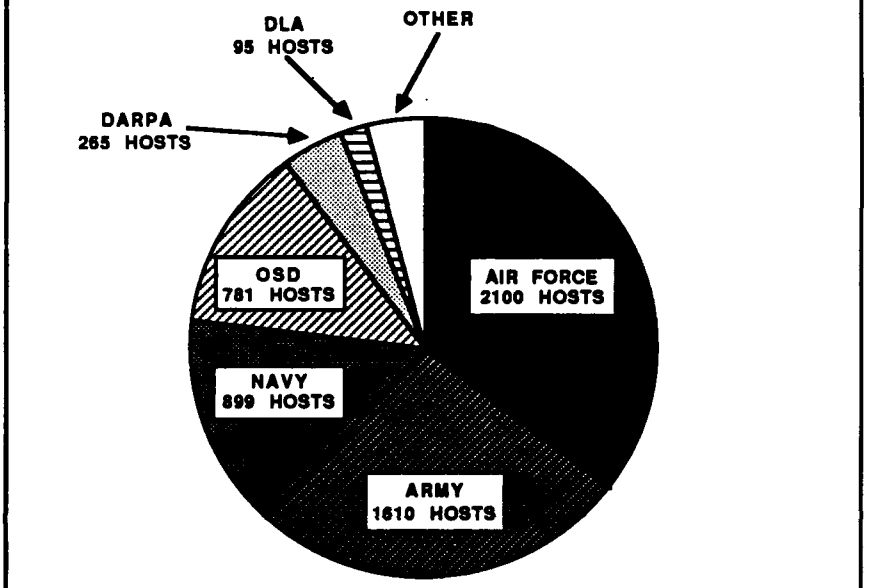
0488/026-003

Attempts to count hosts at various certification levels using the DDN-HOST2 file, indicated no hosts with a certified (i.e., by NCSC criteria) status. This field exhibited an invalid entry, "unknown", or nothing at all. Failure to find any certified subscribers is not surprising, given the expense of the certification process, and the small number of evaluated products currently on the market. Furthermore, discussions with subscribers proved relatively fruitless in this area. Few of the individuals designated as DDN points of contact for their system have substantial familiarity with NCSC publications such as the TCSEC (DoD 5200.28-STD, Orange Book) or TNI (Trusted Network Interpretation, Red Book). Those with familiarity exhibited an incomplete knowledge of the ramifications of such certification on the components of their systems. These findings confront this study with an obvious dilemma: despite the requirements for subscriber certification in the near future, there is no evidence that plans to meet this requirement are widespread.

Additionally, data required to forecast numbers of TGGs to support Closed/Open Community TGGs are not available. This finding does not relegate the Closed/Open Community TGG to non-importance. It appears inevitable that the eventual certification of DDN hosts will necessitate various Closed communities, while others' certifications will create Open communities. Currently, it is not possible to predict when this process will unfold. The DDN-HOST2 file did identify the major agencies having or requiring DDN connections. Figure 3-2 illustrates that 6 major DoD agencies

comprise over 95% of the hosts identified in the URDB. This preliminary round of statistics gathering confirmed that there is a validated, significant requirement for connecting classified subscribers to the DDN. It is also evident that DoD's major services agencies are the primary subscriber community. Establishing this connectivity requirement was the first step in the process of discerning the need for TGGs.

FIGURE 3-2 AGENCY HOST STATISTICS



0488/026-001

3.1.1.2 Identification of Cross-Network Connectivity Requirements

The next step was to conduct a search to ascertain cross-network connectivity requirements between hosts on any of the networks. In the URDB, the DDN-TRAFFIC-MATRIX2 file furnishes "keys" into the DDN-CONNECTION2 file, which in turn furnishes network assignments. In order to form a preliminary identification of subscribers with multiple network connectivity requirements, queries were formulated using these two files. For each record in DDN-TRAFFIC-MATRIX2, corresponding URDB entries (via the field, 'URDB-NBR') for source and destinations were retrieved. Network assignments were obtained, compared, and in the case of two different networks, a report was written. Each report obtained through this process corresponded to a record in the DDN-TRAFFIC-MATRIX2 file that required multiple DDN segment connectivity.

Based upon reports obtained, a number of major DDN systems were noted as potentially requiring multiple DDN segment connectivity. However, the retrieved data displayed duplication (i.e., many identical 'reports' describing the same two systems and networks), and network names that did not satisfy edit criteria (i.e., blank network names; network names not within the stated edit criteria). Disregarding the data just mentioned, the systems listed in Table 3-3 were then subjected to further analysis via the DDN-SYSTEM-MASTER2 and DDN-SYSTEM-NARRATIVE files. In most cases point of contact data or system narrative data was missing. Telephone interviews with the few available points of contact from selected MILNET systems (e.g., IMMIS) yielded little information about potential requirements for multiple segment connectivity or any other TGG requirements. In fact, the only productive contact was with personnel from the AMP-MOD program. (AMP-MOD plans to be the Army's first DISNET system, with an operational capability expected in December 1988.)

The data retrieved through this line of queries proved to be largely unreliable in light of the apparent frequency of edit errors and the inability to generate a significant number of useful contacts with users. This conclusion was supported by a subsequent query, formulated to identify entries in the DDN-TRAFFIC-MATRIX2 file that required multiple security levels, as indicated by corresponding security levels from the DDN-CONNECTION2 file. This investigation produced a list identical to the list for identifying requirements for multiple networks. It appears that this data was not developed by conscientious users aware of current security policies and network architecture limitations. Rather, erroneous data has been generated due to inherent errors in the transcription, editing and entry processes for constructing and updating the URDB.

TABLE 3-3 URDB REGISTERED DDN SYSTEMS WITH CROSS-NETWORK CONNECTIVITY REQUIREMENTS

MILNET SYSTEMS	DISNET SYSTEMS	SCINET SYSTEMS
AMSNET	AMSNET	IDHSC
DAS3	CDNET	IDHSC II
ASIMS	CTASC	DRAGON
CIVPRNET	ASIMS	WINCS SYSTEMS
NAFISS	MAINTDTA	AUTODIN
IMMIS	DAS3	WWMCCWIN
AUTOSTRAD	AMP-MOD	
ACOA	TRALINET	
DARMS		
RCPAC		

0488/026-002

3.1.1.3 Identification of Viable Points of Contact

The next phase of URDB research was predicated on new assumptions that reflected experience gained during the first stages of analysis, correlating information gained from telephone contacts with URDB information. These assumptions are as follows:

- few DDN subscribers have current URDB entries to indicate valid cross-segment connectivity requirements;
- only systems with relatively complete entries in the URDB (completed information regarding points of contact, numbers of hosts and terminals planned, etc.) are likely to provide useful telephone or personal contacts; and
- unclassified DDN (i.e., MILNET) subscribers have little if any involvement in planning applications requiring cross-segment connectivity.

Given these assumptions, additional queries were formulated, to provide points of contact for major DDN "Systems", and for systems where non-zero estimates of host and terminal numbers were found. This search

was limited to non-MILNET and non-ARPANET systems, in accordance with the last assumption. The DDN-SYSTEM-MASTER2 file was accessed according to the following search conditions:

- data field NET-ASSIGNMENT not equal 'ARPA' and data field NET-ASSIGNMENT not equal 'MILNET';
- data field NBR-PROPOSED-HOST greater than ZERO and data field NBR-PROPOSED-TERMINAL greater than ZERO; and
- data field SYS-POC-NAME not equal blank and data field SYS-POC-COMMERCIAL-PHONE not equal blank.

These queries produced a list of systems believed to represent those in advanced stages of implementing or planning major DDN applications. Telephone interviews with points of contact supported this. The appendix following this report summarizes these contacts.

3.1.2 Subscriber Contacts

Once a viable list of contacts was obtained, they were surveyed. The refinement of the list of contacts was an iterative process throughout the period of the contract. Contacts listed as responsible for a particular DDN system change frequently. Given the nature of military assignments, the predominance of military agencies in our list, and the fact that entries made in the URDB are infrequently updated, tracking down tangible contacts was a constant challenge. The format of the survey also evolved as a result of responses received and the level of knowledge of the contacts.

The level to which contacts are informed about DDN security architecture details has been an important factor. They are generally aware that the security architecture currently forbids connection between DDN segments, but have little cognizance of the security approaches to potentially allow such connections. This frequently resulted in a negative response to queries about possible requirements for a TGG. This indicates that user education in this area could result in a significant increase in the potential number of future TGG users. In more than one instance a description of the mechanism and possibilities for TGGs resulted in a rethinking of a contact's needs and requirements.

As the survey progressed, it became useful to classify apparent trends into four categories of systems. These categories were outlined during the early stages of the survey. While more detail has been incorporated into their general definitions, the original categories have held up throughout the performance of contract. Each category and a brief description of the systems that fall into them are presented below.

- CATEGORY A SYSTEMS: These are larger, distributed systems with relatively well defined needs and requirements (e.g., databases requiring access to and updates from field sites). The people contacted for these systems have a better understanding of security requirements and criteria for certification than most contacts in the remaining three categories. They are willing to stand up and say that they have a need for a TGG.

  EXAMPLE: As of November of 1987, ARFCOS was waiting for a SECRET node on DISNET with no firm hook-up date. In the meantime, they have requested an unclassified MILNET node. Both nodes will be at Ft. Meade. Ultimately, they will have 37 field sites, which were being installed at the rate of one/week. They are currently running at system high SECRET, but anticipate being certified MLS. They have requirements for: on-line transaction processing, e-mail, file transfer, data processing, and on-line diagnostics. They are located at Navy sites, Air Force sites and Army sites.

- CATEGORY B SYSTEMS: These systems do not have requirements for the initial implementation of the TGG recommended in this report. However, they have a current or future need for some kind of implementation of a TGG (e.g., a SECRET system-high system knows of other services' systems at the SECRET and TOP SECRET level that require access to it.) Category B systems will be important to future implementations of the TGG with respect to DDN planned product improvements. They are systems that have a current or future need for a TGG allowing access at a level other than UNCLASSIFIED.

  EXAMPLE: AFHRC currently has an operational node on MILNET. They had originally applied for a DISNET node but that meant that field locations would have had to accommodate classified set-ups and they are having a hard time getting KG-84's. Their traffic involves answering queries. They have no incoming traffic. They "might need a downgrader" in the future.

- CATEGORY C SYSTEMS: The contacts interviewed for these systems indicate that they have no real present requirement for a TGG. This was due in large part to a to lack of information and/or knowledge. Description of a TGG evoked a positive response for future need from them in almost all cases. They are the potential future users of TGGs and their requirements,

along with Category A systems, will drive the type and number of TGGs that DDN should plan for, much more than those of Categories B & D

EXAMPLE: AFSAC is a "real" DDN system with hosts and terminals across DISNET. They have two systems running at different classification levels. The point of contact did not see a current or future need to have access to unclassified systems but further discussion indicated that was predicated on disbelief that it would ever be possible. Some familiarity with the Orange Book was exhibited.

- CATEGORY D SYSTEMS: These systems are mission-specific in nature and require little or none of the interoperability possibilities offered by a TGG. They have determined their information sources and the roles of their hosts and their applications do not impact TGG requirements directly. For the most part, these systems are currently on DISNET or have plans to be hooked up in the near future and plan to operate in a system high classified mode. They foresee no need for any interaction with any other systems, especially non-DISNET systems.

  EXAMPLE: The Air Force Space Surveillance Systems are an example of Category D systems. These systems have a well defined mission -- to acquire and process radar data and to send results to command posts. Consequently there is no need nor interest in acquiring information from other DDN segments or even other systems beyond the designated application.

Category D notwithstanding, many contacts recognized possible future implementations of TGGs and expressed a current or future need. Consequently, we have found a significant portion of systems planning to connect to DISNET for whom connectivity with unclassified MILNET is either a requirement or a definite item of interest. It is interesting to note that one of the reasons this connectivity is of importance to users is that many of them have requested nodes on both networks. In many cases this is a result of the long lead times for DISNET nodes. In order to obtain a minimum level of connectivity with the DoD community they then request a MILNET node, which often becomes operational prior to the installation of the DISNET node. By doing this, they are almost certainly placing themselves in a situation where a TGG would be useful for them unless their missions and applications are so distinct that connectivity of the two systems would not benefit them.

As for the other classified nets it is possible to draw many of the same conclusions. Little contact was established with them, however it is highly likely that they may require the same kind of connectivity. To support this, indirect evidence was gained through interviews with future TGG users who believe they know of the connectivity requirements of other users. This desire for connectivity was most frequently expressed in the form of a higher level user desiring access to a lower level system (e.g., TOP SECRET to SECRET).

Tables A-1 through A-4, found in the Appendix, depict surveyed DDN systems, pertinent statistics and relevant TGG status categories.

3.2 Types of Trusted Guard Gateway Required

The information gathered for this contract, including interviews with DDN system points of contact and interviews and discussion with DDN and DCEC personnel, points toward a single basic model of a TGG. This TGG provides interconnection between networks of differing levels of trust, using standard IP datagram processing and routing. It labels data and provides access control (in accordance with the descriptions in Section 4.2), and can support data labeling for all subscribers' applications, since it is an IP gateway. When provided with detailed correspondences between applications and TCP port numbers, it can enforce access control over applications not just limited to TCP, TELNET and FTP. Access controls over specific query/response applications that use TCP could be provided as well.

Interviews with subscribers indicated more reliance upon application-specific use of the DDN rather than the more user-oriented FTP, TELNET, and SMTP. Formalized subscriber requirements, as embodied in Agencies' development programs and registered in the URDB, are not limited to FTP, TELNET and SMTP.

The issue of a TGG between Closed and Open communities within a single segment has not been explored due a lack of available information regarding the certification status of those communities at present. The Closed/Open Community TGG might be different. Perhaps it would need to furnish address resolution data or to act as a packet switch. That would require additional routing mechanisms. Such a TGG might be a gateway with a single network interface. It would provide labeling and access control, but the distinction between levels of trust or Closed and Open could not be made on the basis of network interfaces. Instead, the distinction would have to be made on the basis of the source and destination address. Any data passed into the Open community via this TGG must be labeled as suspect. Access control could be enforced based upon network protocol source indicators as well as IP header and TCP header information. Otherwise a source authentication

mechanism would be required for CLOSED/OPEN communications via the TGG.

This report recommends the use of a single basic model of the TGG. Its use between ARPANET and MILNET, and between Open and Closed communities can be supported with a lighter certification process compared to its certification for use between MILNET and DISNET. However, MILNET/DISNET use has emerged as the best known, best characterized requirement. Developing a basic TGG to meet this requirement, with rich configuration capabilities, will be sufficient for ARPANET/MILNET and Closed/Open Community requirements when they can be known in detail.

3.3 *Conclusions*

3.3.1 Direct Results

As the survey continued, a richer field of contacts was developed as those interested in TGGs pointed to others who had similar requirements. Through this process, a representative sample of the complexion of systems on or proposed for DISNET was obtained. This sample is characterized by users in advanced stages of planning. It does not appear to be biased with respect to service, agency, nor types of applications supported.

It is not currently possible to adequately forecast requirements for the systems classified at the TOP SECRET or SCI levels. Most of the information gathered concerns DISNET subscribers. Telephone contact is anathema to many of the people responsible for TOP SECRET and SCI systems. Frequently, reference is made to higher echelons that are difficult to contact. Additionally, the number of TOP SECRET and SCI systems represent a small percentage of the total user population.

Based upon the detailed interviews conducted with primarily DISNET subscribers during the contract effort, it is estimated that 42% of the systems planning to use the DDN have definite requirements for a TGG (Category A), 15% have definite interest in capabilities to interoperate with less "trusted" DDN segments of differing trust levels (Category B), and 24% have missions for which TGG-furnished interoperability is of little interest (Category D). 19% of the systems may have a requirement for TGGs now or later but better education and further investigation would be needed to discern their actual needs. These percentages are based upon a categorization of responses from a set of 35 points of contact, discussing 26 distinct DISNET subscriber systems. The appendix at the end of this document provides detailed information on these systems and points of contact.

3.3.2 Indirect Results

The discussion of the user survey portion of this contractual effort identified several issues that bear consideration now and in future work regarding the TGG. These considerations range from the kinds of systems that are anticipating hook-up to the DDN in the near future to how DDN will manage information regarding these potential users and communicate with them.

Regarding the kinds of systems that anticipate connection to the DDN, several observations can be made. The issues of LANs and TACs on the DDN are two areas that could not be adequately addressed within the scope of the user survey though when possible, interviews were conducted to discern any relevant information concerning them. The best insight into both of them was provided by a study of the current networking technology being employed on the premises of military complexes, conducted by BBN in 1986[13].

One of the recommendations to DCA coming out of the Premises study by BBN is that DCA look at TAC, mini-TAC and TACACs functionality and distribution. These should become less important as Premises systems (consisting primarily of LANs) develop. Ultimately, they will serve only to provide common user dial-in ports. They must also be upgraded to support ISO protocols. The same recommendation, a close examination of functionality and distribution, should be followed regarding LANs. The user survey confirmed that LAN technology at these sites is proliferating at a rapid rate, frequently without a systematic approach to an ultimate interface into the DDN. Significant changes to host and terminal counts in the URDB also support this. Since URDB statistics tend to lag behind the actual occurrence of the trends, keeping track of these issues and how they affect the topology of the DDN could be a major factor in the distribution of TGGs across the DDN.

Finally, in discussions with contacts for the various systems, mixed responses were received regarding levels of communication with DCA and DDN planners and the usefulness of URDB registration. The comments ranged from frustration with sending in updates to the URDB that never seemed to appear in the system, to gratification that the information was being used by DCA for planning purposes. As a sidelight to the main thrust of the user survey, it became apparent that these contacts welcomed the continuity of talking to someone more than once over the course of a six to nine month period about DDN matters. As in the case of the systems classified in Category C (unsure of requirements, in need of some level of

---

[13]DDN Premises Technology Study, BBN, 1986

information), this kind of follow-up approach could potentially provide continuing insights into the changing complexion of the DDN.

4.0 TGG Requirements Definition

This section discusses and evaluates alternative approaches to TGG protocol functionality -- how the TGG should perform in order to best fulfill its network role. Particular operational models are discussed in Section 4.1, and a recommendation is introduced in Section 4.2. Computer security (COMPUSEC) issues are presented in Section 4.3 with tradeoffs between security and functionality addressed in Section 4.4. Section 4.5 summarizes specific TGG requirements and issues relating to multi-homed hosts serving as virtual TGGs are discussed in Section 4.6.

4.1 TGG Network Role Alternatives

Three operational models of TGG processing were initially considered. These correspond to the protocol layers that need to be considered when enforcing the basic requirements of data labeling and access control. The three models are:

1. An IP gateway that performs operations on IP datagrams using data contained in IP headers;
2. A transport level gateway that performs operations on TCP segments using data contained in IP and TCP headers;
3. An application gateway that performs operations on application data.

These operational models have counterparts in real systems. IP gateways comprise the backbone of the DoD Internet, and application gateways are under development sponsored by NBS and DoD to support transition to the ISO protocol suite. The models represent three isolated possibilities, but do not encompass the entire realm of possible operational models. They are presented for the purpose of discussion of gateway operations and security implications at each protocol level.

4.1.1 IP Gateway

An IP gateway would operate much as a conventional gateway, receiving and relaying IP datagrams in accordance with information contained in IP headers and in internal routing tables. The basis of data labeling would be the TGG's network interfaces. When the gateway is initially configured, each interface is designated as high side or low side. High side refers to the connected network with a greater degree of trust or with more sensitive data. Data entering from the low side bound for the high side must be labeled by

the gateway to indicate that the IP datagram address may be inaccurate and has not been authenticated. Special action may be taken by a TGG upon receipt of a datagram already labeled by a TGG.

Access control that can be performed solely at the IP level is on the host-pair basis, since each IP address corresponds to a host. It is possible to perform access control on the next higher layer protocol field such that specific transport protocols could be excluded (e.g., rejecting UDP and passing TCP). This form of access control has limited significance in the DoD Internet, since most of the applications use the same transport protocol, TCP.

4.1.2 Transport Gateway

A transport gateway would perform data labeling and access controls upon data units (Transport Protocol Data Units--TPDUs) exchanged between end systems' (hosts') transport protocol implementations. A practical method for performing this is to place rudimentary transport protocol implementations for each half of the connection in the TGG. These would reassemble IP datagrams into segments. This approach precludes any adaptive dynamic routing or multipath routing through multiple TGGs. The TGG would be a fixed endpoint for both halves of the transport connection for the duration of the transport connection.

TPDUs travelling from a low side network to a high side network would be labeled in accordance with the data labeling policy.

Access control based on specific applications would be possible. In the case of TCP, port numbers (and possibly IP address pairs) could be checked against an access control database with prohibited actions resulting in dropped TPDUs or rejected connections.

A transport gateway would be suited well for a guard application to allow unclassified systems to send real data to classified systems. A problem that naturally arises in this scenario is the use of reliable protocols. Often, the classified system cannot be trusted to send a simple acknowledgement of the unclassified data. A guard gateway could form two transport connections between the two systems. Based on its own trustedness, unclassified data could be upgraded, and acknowledgements could be provided to the sender. The acknowledgements would originate from the gateway instead of the classified system. This approach might still allow a low bandwidth channel for application control information.

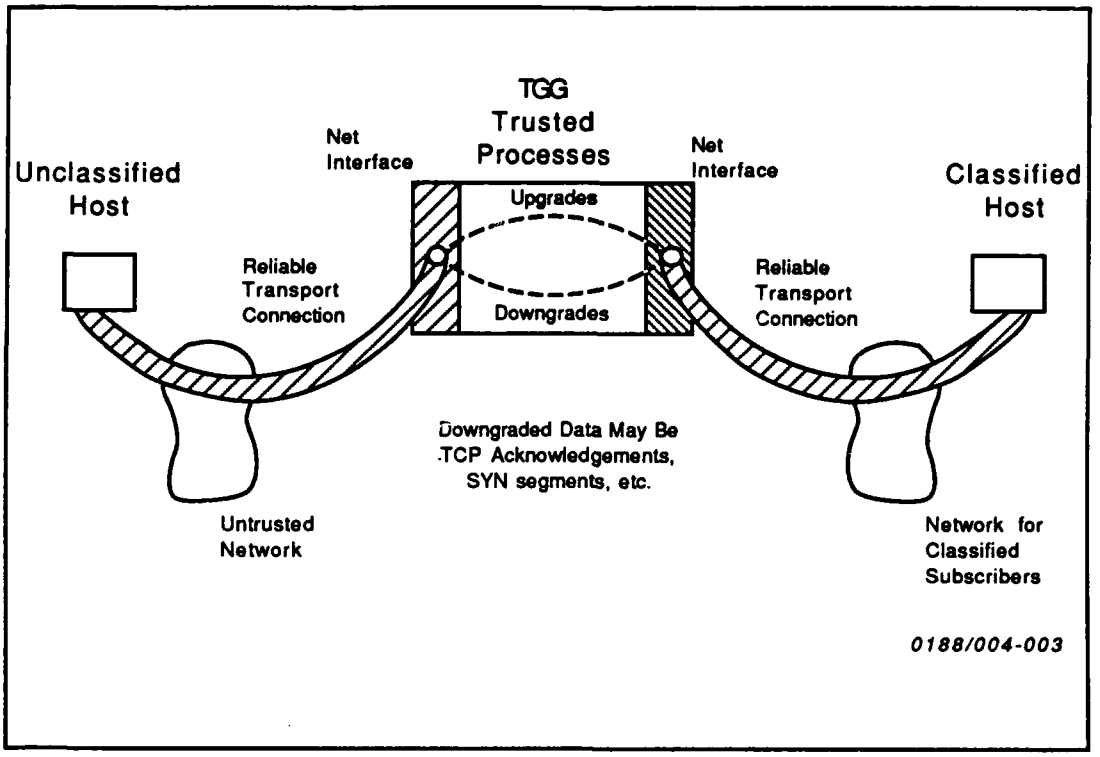


Figure 4.1-1 TGG Transport Gateway Model

4.1.3 Application Gateway

An application gateway would perform data labeling and access controls upon protocol data units (PDUs) exchanged by end systems' application protocol implementations. Application protocols (e.g., TELNET, SMTP and FTP) exchange varied types of PDUs, but the concepts of control messages and data messages are retained. The gateway would need to reassemble IP datagrams into segments and ultimately process segments into application protocol data units. This would involve end-to-end operation similar to message switching as used in previous generation networks such as AUTODIN.

Data coming from low side networks would be labeled to reveal its origin. No particular labeling method is proposed here, but it should be noted that application level labeling is more complex than in the cases of transport and IP gateways because of the existence of different application protocols with differing data unit structures. In contrast, IP and TCP data unit labeling can be uniform.

Application-level gateway operation would support some access control to the user or process level. User process identifiers, as found in the application control data, with entries indicated as "do not allow", would result in the gateway rejecting the message. TGG access to individual

application messages would also permit the restriction of particular application functions. (e.g., FTP directory commands, the transfer of binary or image files, or SMTP verify user (VRFY) commands).

4.2 TGG Approaches

All three distinct operational models have both advantages and drawbacks:

1. IP Gateway: simplicity versus poor access control granularity;
2. Transport Gateway: moderate access control granularity versus difficulty of monitoring data flow; added complexity without truly enhanced functionality; supports limited upgrading;
3. Application Gateway: very good access control granularity versus delay and problems associated with transport gateways.

To securely provide the required user services, the TGG will be based around an augmented IP gateway. The TGGs will operate primarily on IP datagrams, but will also operate on extracted limited TCP header data.

4.2.1 IP Gateway Basis

The TGG described here is fundamentally an IP gateway, processing IP datagrams. It does not aggregate these datagrams into any higher level protocol data units for processing. The selection of an IP gateway is based on:

1. the desire to minimize complexity;
2. the desire to maintain dynamic internet routing;
3. the sufficiency of access control at the gateway level (as described in Section 4.2.3).

The finer granularity access control provided by an application gateway is inconsistent with a centrally administered system and, rather, should be provided by end systems.

4.2.2 Data Labeling

The TGG performs data labeling on the basis of its high side and low side network interfaces. Any data coming from the low side network interface to be relayed into a high side network must be labeled. Figure 4.2-1 provides an illustration of this.

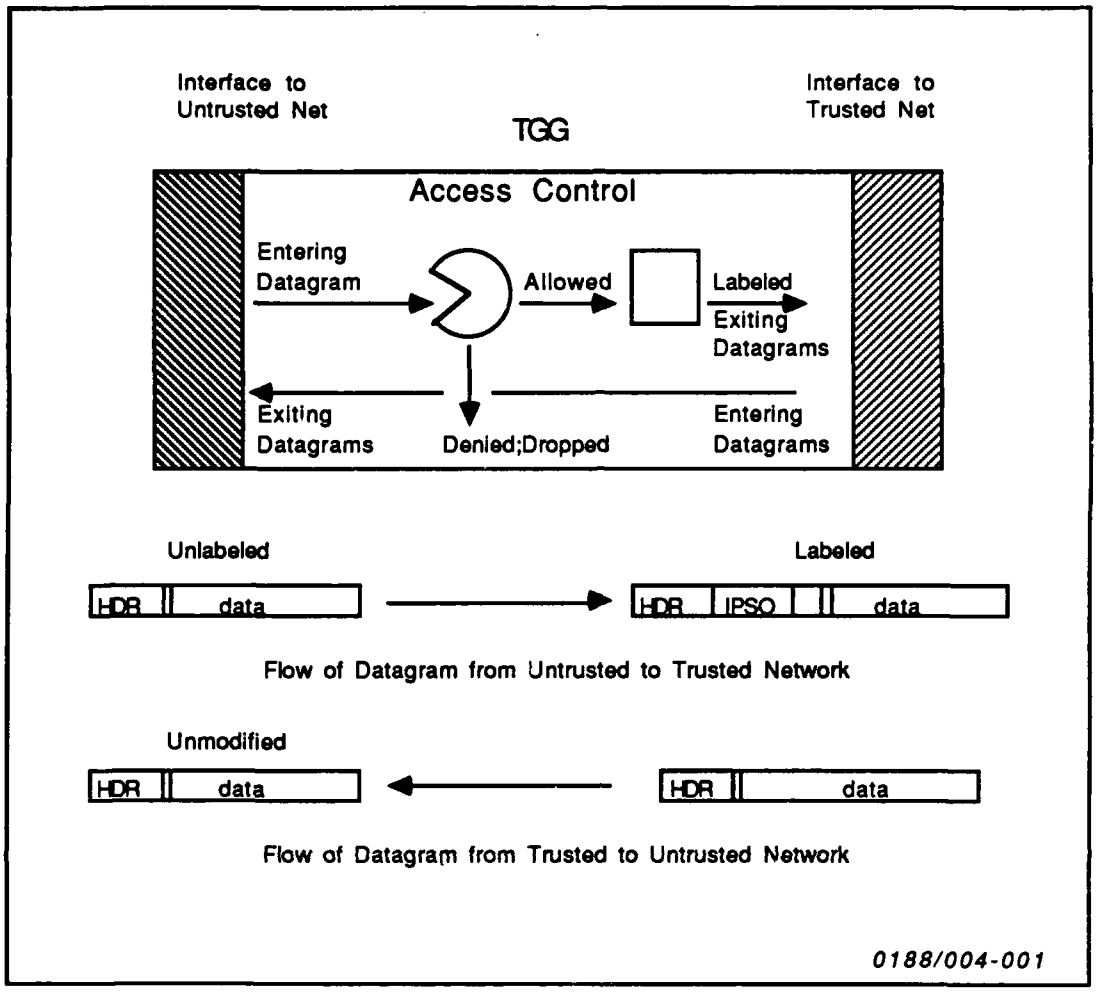


Figure 4.2-1 TGG Access Control and Labeling

Three locations for data labels within the IP datagram header structure have been identified:

1. the accreditor bit fields within the IP Basic Security Option (IPSO, option 130): this field is easily extended and because there are currently less than seven authorities, bits 4-7 are unassigned. The formal, organizational significance of the accreditor bits may make this choice unattractive;
2. the extended IPSO (option 133): this field offers a convenient position in which to encode labels indicating the level of trust in the data origin. Use of the IPSO (Basic or Extended) for labeling would permit the BLACKER system, if desired, to enforce access control based on these labels;
3. an as-yet unused flag bit in the main IP header, bit 0 of the seventh IP header octet: this bit offers a convenient and highly

efficient means of labeling data as high or low; however, it provides only binary distinction and also may preclude a later use within the IP standard applicable to all IP implementations.

Both the MILNET/DISNET TGG and the ARPANET/MILNET TGG can rely on their own configuration to distinguish between low side and high side data origins. This problem is more difficult for the CLOSED/OPEN TGG, which may have a single network interface to a packet switching node. In this case, there is a threat of IP address spoofing. However, a useful policy is to regard any incoming datagram addressed to a host within the Open community as being of doubtful origin. This policy for the CLOSED/OPEN TGG can allow specific software design for all three TGGs above the network interfaces to be identical.

4.2.3 Access Control

The TGG performs access control on the basis of IP header information and, optionally, on the basis of TCP header information. Although complete TCP data streams cannot be monitored, an effective degree of access control can be implemented nonetheless. TCP port information indicates the application protocol involved. The TCP port numbers for SMTP, TCP and TELNET are widely known. More flexible, user specific access control at TGGs will require more detailed lists of acceptable and unacceptable TCP port numbers. Using these port numbers can readily prevent prohibited application PDUs from reaching their destination. Access control should be enforced upon TCP connection initiation (SYN TPDUs). Access control is actually enforced on every TCP TPDU; however, detection of an invalid TPDU other than a SYN indicates a larger problem. Given this approach for access control, the detection of an established TCP connection in violation of the access control list indicates a serious security problem. The connection may have been established through a back channel via another gateway, but has temporarily passed through the TGG. Such an event must be communicated to a higher authority.

Datagrams containing TCP port numbers corresponding to "do not allow" entries can be dropped, and a security-relevant event can be recorded. This prevents unwanted TCP connections from low side networks. IP headers are checked to determine if the datagram is a fragment other than the first. For such a datagram the TGG will not look for TCP header information and will operate only on the IP header information.

4.3 COMPUSEC Issues

4.3.1 COMPUSEC Certification Level

The TGG is intended to be an integral part of the DDN and the DDN security architecture. As such, it must provide an appropriate set of security features with a corresponding level of assurance. The nature of the TGG's role places the assurance focus on COMPUSEC issues. In defining requirements for the TGG, it is therefore necessary to select an appropriate COMPUSEC certification level as defined in the Orange Book. The selection of a target certification level is based on the security services provided, the sensitivity of the data processed, the clearance of users, and the operational environment. For any selected certification level the criteria must be interpreted for a network environment with specific sections taken as is, deleted, or adjusted. This process has been applied in the Trusted Network Interpretation (TNI) which serves as a basis for performing the tailoring of the TCSEC criteria for the TGG. A discussion of the applicability of the TNI to the TGG can be found below.

The TGG, as defined in this document, is principally an access control device. In the scenarios identified so far, the TGG operates with interfaces at equivalent security level ranges and performs discretionary access control functions. For the principal applications, connecting the ARPANET and MILNET and connecting the MILNET and DISNET, the TGG handles only unclassified information. While the TGG must not adversely effect integrity or assured service characteristics in the DDN, it does not have a primary responsibility in these areas. The TGG provides an identity based check on access to resources between security environments and provides additional security functions such as auditing and labeling needed to support the primary function of access control. Mandatory access checks are the responsibility of, and are performed by, the systems being connected (e.g., in the DISNET, this is performed by the BLACKER system).

Another factor in considering a certification level is the environment in which the system will be operating. For the TGG, while the device will only handle unclassified information, it will be located in a secret cleared facility. Further, TGGs are expected to be dedicated applications running on computer systems without interactive users and without user programs or other applications. The only human interaction will be remote monitoring and maintenance by cleared operators and local maintenance by cleared personnel. This limitation reduces the risk of exploitation through user activities involving penetration, circumvention, or covert signaling. The remote monitoring and control capability includes the update of the access control database. Depending on the development approach eventually adopted, it may also be possible to develop the TGG with cleared individuals.

One of the critical aspects in selecting the certification level of the TGG is the subject of control traffic. As discussed above, the TGG is viewed as a single level device. While this assumption is largely unchallenged with respect to user traffic, potential problems exist with respect to control traffic. Control traffic can be divided into four categories. The first category is gateway support, traffic in support of the gateway function exchanged between gateways and between gateways and hosts. This category includes gateway routing exchanges, diagnostic messages such as ICMP, and other gateway control messages including reachability or liveness. The second category is software maintenance including the downline loading of complete software images as well as debugs and patches. The third category involves operational information. This is information that configures the gateway in terms of operational parameters, interface information, hardware control, enablement and reset, and access control permissions. The fourth category is monitoring. Monitoring includes the periodic, or on demand, reporting of statistics, performance, and security audit information.

While all of these remote control functions must be subjected to strong authentication, the sensitivity levels may vary. The relative sensitivity of the control traffic is based on the communication with other entities, the level of trust of those entities, and the types of information or commands exchanged. For the TGG, the other entities involved include other gateways, hosts, and network control centers. These entities may be situated on any of the networks attached to the TGG. The particular case of concern is the MILNET/DISNET TGG. The assessment of this issue is complicated by the lack of definition in the gateway structure and the monitoring and control approach within the DISNET. For monitoring and operational control traffic the problem is that of having a central facility capable of interfacing to individual components at several different levels. The alternative to an MLS monitoring center is to rely on all monitored elements to be A1 certified (to cover the full range of monitoring and user data) or to have several independent monitoring centers for each security level and combination of security levels.

The MLS character of the DISNET will pose serious challenges to the current gateway algorithms by adding an extra dimension, that of security classification levels. Reachability information will vary according to the classification levels of networks, gateways, and individual datagrams. The sensitivity of that information, the responsibility for filtering the data, and the algorithms involved are all unspecified at this time. The issue is how to deal with reachability and routing information for networks with classification ranges that only partially intersect with or do not intersect with peer gateways. In figure 4.3-1, consider the case of GW1, a likely configuration for the TGG. It can potentially exchange routing information with GW2 and

GW3. Because the classification range of GW2 (S-TS) does not intersect with GW1 (U), network N2 should prevent any exchange between them. Considerations for GW1 and GW3 become more complex. For a host on N4 to communicate with a host on N1, both of which are unclassified, GW3 must advertise a route. The problem relates to what information GW3 sends regarding N7 (S), N3 (U-S), or N5 (S-TS). Since information on these networks may be deemed secret, the exchange of such information would require GW1 to be MLS. Alternately, since authorized communication with those networks cannot occur, GW3 could provide some degree of filtering. To permit a definitive assessment of the impact of MLS gateway routing on TGG certification, resolution of these issues for the DISNET must be reached.

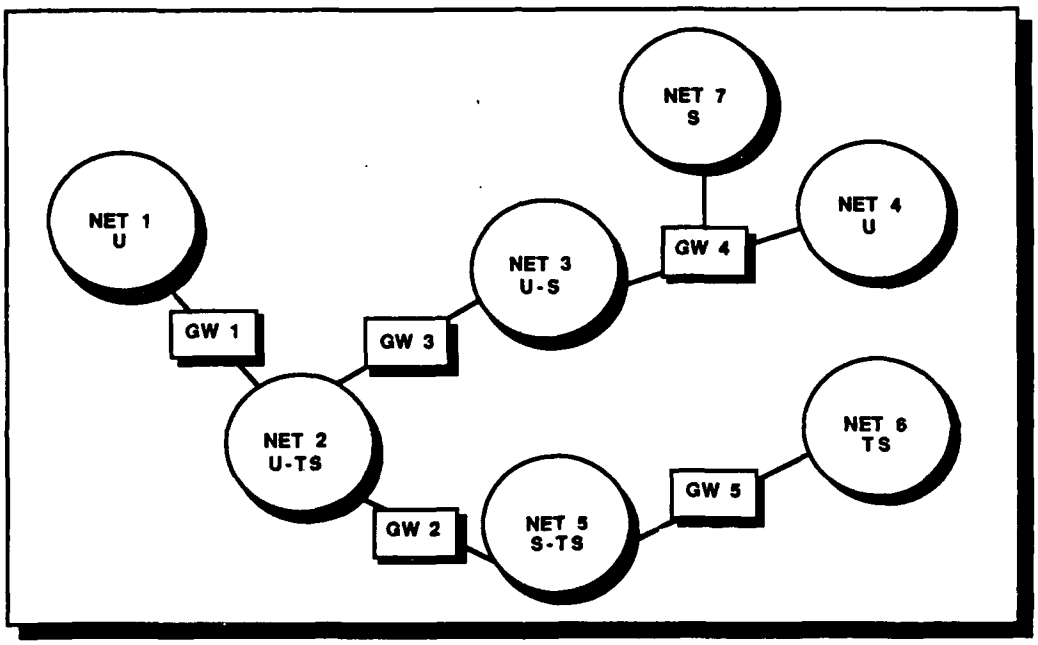


Figure 4.3-1 MLS Gateway Routing Problem

For the TGG, it is best at this time to assume that MLS devices within the DISNET will be capable of recognizing the TGG as a single level unclassified device and preventing any classified information from reaching it, thus relieving the TGG of the responsibility for providing mandatory access control. The requirements for certification of the TGG will be based on the environment consistent with unclassified and FOUO user and control data. The remainder of this discussion will operate under that premise. If the future design of the DISNET monitoring, control, and gateway systems requires multilevel processing within the MILNET/DISNET TGG, then the certification requirement for the TGG must correspond to the levels to be processed. If the data is deemed secret only, then a full B2 system would be mandated. If TOP SECRET or SCI information is involved, then an A1 or

higher system would be needed. The implications of these issues on all network elements must be considered as the DISNET design and architecture evolve.

Of the applications for the TGG, the MILNET/DISNET TGG is the most sensitive The Closed/Open Community TGG and the additional TGGs described below will be addressed separately. In the MILNET/DISNET application the TGG processes unclassified information, FOUO information, and other sensitive unclassified information. No classified information is handled. All personnel with physical access to the TGG are cleared. The environmental guidelines (CSC-STD-003-85, Yellow Book) call for a B1 system for such an application. Although protected by an A1 access control system in the DISNET (BLACKER), the sensitivity of the more classified information accessible through the DISNET along with the issue of control traffic suggests that a higher than mandated certification level for the MILNET/DISNET TGG may be appropriate. This is particularly focused on the greater assurance provided at the B2 level through improved specifications, hardware architectures, testing, etc.

Some of these assurance techniques can be provided as enhancements to a B1 certified system without requiring all of the B2 features. Items such as strict configuration control and improved testing are likely and natural requirements for a TGG. Some of the more rigorous specification, formal modeling, hardware architecture, and extensive labeling requirements are less appropriate and more burdensome on the TGG.

The choice of a B2 target level, while desirable, needs to be balanced against pragmatic considerations. While higher levels provide security advantages, these advantages come at the expense of higher cost, prolonged schedule, potentially reduced performance, restricted technology availability and selection, and program risk. These factors are of serious concern in considering how the TGG effort should proceed.

Based on these arguments, and subject to the assumptions on control traffic stated above, the TGG should meet the requirements for a B1 system, as interpreted for a network device, and supplemented by additional selected B2 level criteria. The additional requirements include rigorous configuration control and management, enhanced security testing, and a trusted path (i.e., authentication of control traffic). Enhanced security testing refers to increased resources applied to the testing of TGG operation and security properties rather than to B2 testing requirements. The strict B2 requirements would be applicable only with the adoption of the complete B2 requirements. The application of the system architecture requirement for B2 systems will require a tradeoff analysis as part of the consideration of developmental alternatives.

The TGG is also being considered for environments involving classified information, as between Closed and Open communities in the DISNET or between the DISNET and LANs. In such a case the TGG must be certified to at least the highest certification level of the environments connected.

4.3.2 Application of the TNI

The preceding discussion concerning a COMPUSEC certification level is based on an analysis of the DDN security architecture and on the application of principles and guidelines contained in the Orange and Yellow Books. The Trusted Network Interpretation (TNI) addresses the application of Orange Book principles to a network environment. The TNI consists interpretations of the detailed requirements in the TCSEC that are primarily confidentiality related, broad descriptions of other service (primarily integrity and assured service), and rules for the evaluation and interconnection of components.

The most directly applicable aspect of the TNI is the interpretation of Orange Book requirements. The Orange Book requirements are focused on general purpose operating systems. As a consequence, the notions of users, subjects, objects, etc., must be adapted for a network environment. The TNI provides an agreed upon set of such adaptations and eliminates the need for the TGG to provide its own interpretations.

The TNI discussion of additional services provides little assistance in addressing TGG requirements. While some of the services could be included in the TGG, the descriptions in the TNI are broad, generic treatments. The TGG requirements already provide a more detailed discussion of these issues where appropriate.

With respect to component and interconnection issues, the TGG could be considered as a component of the DDN rather than as a system. As such, it would probably be classed as an IAD (identification and authentication, audit, and discretionary access control) component with an associated certification range of C2+. Because the security functions performed by the TGG are well defined and self contained the TGG can equally well be evaluated with the TNI system criteria.

One potentially relevant aspect of the component connection rules is the issue of cascading; the concatenation of more than two security environments. A problem can occur when a series of system interconnections are considered in isolation without regard to the transitive effect on the overall network system. In such a case the interconnection elements, such as gateways, may need to consider the entire system security range rather than the range of the directly connected segments. The cascading situation for the TGG involves the interconnection of the ARPANET,

MILNET, and DISNET. The implications for the TGG are that both the ARPANET/MILNET and MILNET/DISNET TGGs should be certified to a common level which accommodates unclassified to FOUO information (or higher as discussed above).

For the TGG, the TNI provides both the set of specific evaluation criteria for a B1 class network system and a set of topics for consideration in defining the security requirements and architecture for the TGG.

4.4 Tradeoff Considerations

The proposed TGG operational model affords both interoperability and security between networks or communities with differing security characteristics. However, functions and services NOT performed by the TGG should also be considered: (1) the TGG does not enforce confidentiality among multiple levels of data sensitivity; (2) the TGG as proposed does not provide for interoperation between hosts at unequal security levels, even for upgrades only; and (3) the TGG does not restrict protocol functions within an application.

The security services of the TGG do provide protection against denial of service threats to the users and hosts on high side networks.

- The data labeling capability guards against spoofing attacks and alerts receivers to the untrustworthiness of data. Hosts can adopt a variety of responses to this alert.
- The access control capability helps to guard against denial of service due to flooding attacks. The access control function limits the damage from such an attack on the TGG to the availability of the low side network interface. The high side network is not heavily affected by these flooding attacks.
- Protection against flooding is also provided by flow or event-count thresholds that can be set in the TGG. For example, datagram counts between some host pairs could be monitored.
- The TGG protects sensitive data simply by prohibiting some types of access from the low side segment, (e.g., TELNET operation.)

The TGG provides passive support for the end-to-end confidentiality and integrity services in the DDN. These services are supported cooperatively throughout the protocol layers at both intermediate and end systems. The passive support in the TGG is represented by the confidence that the TGG will not maliciously modify or compromise user data.

As discussed above, the TGG defined in this report does not support the upgrading or downgrading of data. Downgrading requires a determination that information which is labeled as classified is, in fact, unclassified. Such a determination must be based on a knowledge of the context of the application and current classification guidelines. Attempts to provide a downgrading guard based on a keyword or label search have proved unsuccessful (as with the FORSCOM Guard). A successful guard also requires a close interaction between users in a well defined community and the designers and operators of the guard system. All of these factors make the inclusion of a downgrading capability in the TGG impractical for the general case. General purpose downgraders remain a research issue at this time.

Upgrading is also discussed in Section 4.1.2 on transport gateways. While upgrading is simpler since giving unclassified information a higher label does not pose the risks of downgrading, the structure of the DDN introduces complications. Passing data in the principal applications and transport protocols requires two-way exchange of control information. The control information passed from the high side host to the originating low side host would require at least a limited downgrading capability. Such functionality is also inconsistent with an IP gateway. As discussed in Section 4.1, upgrading requires at least a transport relay and most likely an applicatic relay.

A possible special case which may be practical is an upgrading mail relay. This relay would be substantially different from the TGG described in the rest of this document. The upgrading mail relay could receive mail from a low side host, acknowledge and process it, and then send it on to the high side host. No return traffic would be permitted. Access to this service could be restricted based on an access control list and labels could be placed in the mail header.

4.5 TGG Requirements

The preceding sections have discussed issues and presented alternatives associated with defining TGG requirements. The recommended approach balances security requirements, operational requirements, feasibility, and flexibility. The particular functions invoked in a given deployed TGG will depend on static configuration information and dynamic access control tables. This flexibility will allow a common TGG to be used in all scenarios and for the access policy and security functionality of the TGG to evolve with the overall DDN policy and the DDN security posture (other security systems, certified hosts, certified network components). Based on our user survey, the selection of permitted applications (mail, file transfer, etc.) is especially variable. While the default requirements may be relatively restrictive, the

TGG must be able to accommodate custom applications and interactive traffic for some subset of users.

The following paragraphs define the high level baseline requirements for the TGG:

1. The TGG must be capable of performing all the standard functions expected of an IP gateway for the DDN.
2. The TGG must support network interfaces for ARPANET, MILNET, and DISNET as well as for the BLACKER Front End.
3. The TGG must label all datagrams passing from a low side segment to a high side segment. The label will be placed in an extended IPSO field (IP Option 133). Because network segments are concatenated, a TGG may receive a datagram already labeled by another TGG. Depending on configuration information a datagram already labeled will be:
    a) audited and discarded, with a message sent to the source,
    b) passed without modification subject to other access control checks,
    c) be relabeled with a different or supplementary label.
4. The TGG must be able to limit the flow of datagrams from a low side segment into a high side segment. This limitation will be based on a TGG's configuration. The TGG will keep counters for any limitations and discard datagrams which exceed those limits. Thresholds may be set for:
    a) total number of datagrams across an interface,
    b) total number of datagrams from a particular source address,
    c) total number of TCP connection requests (as reflected by SYN TPDUs),
    d) number of access control rejections (this will shut down an interface).
5. The TGG must enforce access control rules on every datagram. The TGG will maintain an access control database which defines permitted and restricted datagrams by interface and by source address. The following fields are potentially subjected to access control checks:

a) IP source network number, restricting where traffic can originate;

b) IP source and destination addresses, restricting which host pairs can communicate;

c) IP protocol field, limiting the transport protocols that are allowed (such as prohibiting UDP applications);

d) TCP port field, identifying which application is being used and restricts the use of mail, file transfer, virtual terminal, etc. This field also indicates the originator of the application and can restrict application direction. TCP port access control rules are maintained on an interface and on a source and destination address basis;

e) IP security options as discussed in the requirement for labeling.

6. The TGG must support remote monitoring and control. The formats, mechanisms, and protocols for monitoring and control should be consistent with evolving standards for network management (especially those being developed for DDN). Monitoring and control functions include:

a) status and health reporting,

b) remote tests and diagnostics,

c) security audit reports,

d) control of TGG configuration parameters identified above,

e) control of the access control database described above.

7. Assurance must be provided that the TGG securely performs these functions, protects data, and cannot be circumvented. This assurance is provided in part by COMPUSEC Certification. Based on the environment, the DDN plans, performance requirements, and technical availability, the TGG should be certified to a B1 level. The selection of the B1 level and its interpretation are based on the assumptions previously discussed in Section 4.3.

8. The baseline TGG configuration is as follows:

a) label datagrams with extended IPSO and pass datagrams that are already labeled,

b) no flow limitations across any interfaces,

c) access rules are enforced on IP protocol field and TCP port field for all datagrams across an interface. Only TCP is allowed and only mail and file transfer applications are supported.

4.6 Multi-Homed Host Considerations

A multi-homed host is a subscriber machine that has interfaces on two or more networks. This section discusses the implications of a multi-homed host in the DDN context and identifies threats and countermeasures. This section also identifies additional security requirements that should be met by subscriber hosts contemplating a multi-homed configuration between two networks of distinct trust levels. In order for TGGs to effectively provide security, ALL paths between segments (e.g., ARPANET and MILNET) must be secured. While any such configuration except for the TGG are precluded in the current DDN architecture, this discussion serves as a background for possible evolutionary paths the DDN may take.

4.6.1 Equivalence to Trusted Guard Gateway

A multi-homed host attached to networks of differing security characteristics has a role equivalent to a TGG. Such a host can act as an IP gateway in addition to providing services for users directly logged into it. IP datagrams can originate within the low side network, be routed through the multi-homed host, and subsequently be relayed to a high side network, and vice-versa.

4.6.2 Security Concerns

A multi-homed host could, in principle, be a vehicle for attacks perpetrated from a low side network, with the attacks including spoofing denial of service by flooding. Any users of a multi-homed host may have the capability to define and execute processes that in turn communicate over available network interfaces. Also, users may be capable of communication via IP datagrams.

Users from a low side network, or a multi-homed host, may mount attacks against a high side network by opening TCP connections or, if unsuccessful, by sending IP datagrams in sufficient quantities so as to disrupt services within the high side network. Similarly, TCP and application-level connections may be opened with false identifiers to attempt transactions that would otherwise be unauthorized. Such processes operating from a multi-

homed host, gaining access to a host within a segment, would be indistinguishable from processes and users belonging to that host.

4.6.3 Countermeasures

4.6.3.1 General Considerations

The countermeasures for these attacks include measures described for the TGG, as well as additional measures for the control of and access to resources within the multi-homed host. The multi-homed host must be capable of labeling data travelling from the low side network into the high side network. In addition, the multi-homed host must be capable of performing discretionary access controls to selectively or comprehensively prohibit user activities between the attached networks.

In the case of the TGG, these requirements apply to the only service the machine performs: switching IP datagrams over multiple network interfaces. These countermeasures protect against a limited set of attacks that could be mounted by processes assuming a basic gateway between themselves and the target network.

4.6.3.2 Specific Security Requirements for Multi-Homed Hosts

A multi-homed host must therefore limit the degree to which users accessing it via low side networks can execute processes and otherwise control its resources. It must curtail their access to software development (via software tools, etc.).

The capability set of the users accessing a host from the low side network must be limited. These capabilities are primarily in regard to process execution, but to support this, read and write capabilities will also be necessary and must be limited. Any data relevant to the identification of processes must be read- and write-protected. Write access to the high side network interface must be protected as well. Process class identifications must always be bound to the network interface identification (e.g., DISNET, MILNET) to reduce the possibility of these safeguards being bypassed as a result of masquerading. They must be enforced over the objections of users accustomed to mobility and logging on from different sites.

The above countermeasures must be implemented by hosts that are multi-homed on networks with differing security characteristics. The existence of such a configuration may pose a threat to DoD confidentiality requirements as well as posing significant threats to the assured service within the high side network. The countermeasures aim to limit the degree to which such threats could be mounted through a multi-homed host.

5.0 Technology Assessment

In this Section, commercial and government gateway products are surveyed, and their applicability to the acquisition or development of a TGG is noted. There are no current gateway implementations entirely suited for use as TGGs. This is not surprising, because the TGG requirements are new and have not surfaced in commercial and government gateway designs. The TGG, as presented in this report, represents only a modest functional departure from commercial and government-sponsored gateway implementations. Therefore, the prospects for implementing and acquiring a TGG by 1990 are good based on the experience gained to date with gateway implementations.

Section 5.1 reviews the important distinctions and differences betwee existing designs and the TGG and notes the implications of using existing gateway implementations as the basis of TGG development. Section 5.2 discusses TGG software issues, with a view toward the feasibility of developing specialized TGG software. Even though TGG requirements are not radically different from standard DoD gateway requirements, software development and certification are major acquisition expenses. Section 5.3 concludes that a TGG can be developed from current technology, and that its additional security mechanisms, functions and interfaces represent a significant certification effort.

5.1 Overview of Existing Gateway Implementations

This section discusses the better known gateway implementations with respect to their salient features and to their potential for migration to a TGG role. With the exception of the use of parallel processing, as seen in the Multi-Net and BBN Butterfly gateways, there is some degree of convergence and similarity in gateway hardware architectures. Recent gateways have been based upon the Motorola 68020 or processors of similar capability. Network interface processing is performed under the control of separate, independent CPUs. Primary memory sizes are in the megabyte range. Many gateways make no use of secondary memory and rely upon software uploading and downloading instead. On the other hand, software implementations are more distinct among gateway implementations with regard to both features and performance. For example, differing commercial gateway products may or may not offer particular routing protocols and network management capabilities.

5.1.1 The FACC Multi Net Gateway

The Multi Net Gateway (MNG) was developed by Ford Aerospace Communications Corporation (FACC) under RADC sponsorship. The MNG

allows users at multiple levels of classification to exchange data over both protected networks and public networks, using cryptographic RED/BLACK separation for the latter. A multi-level secure (software/hardware) operating system enforces confidentiality among user communications within the gateway.

The MNG hardware architecture uses multiple Zilog Z8001 16-bit microprocessors. Processors run an MLS kernel which can run tasks at multiple security levels. The multiple processors communicate over a dual system bus. The security policy is enforced by the software design and at runtime by an active bus monitor. This hardware architecture can process approximately 150 datagrams per second, if no encryption functions are required. With encryption, the rate is 50 datagrams per second.

The MNG has been under evaluation by the NCSC, with the intent of achieving an A1 rating. The requisite formal, mathematical models for the certification are still under formulation. As of this writing, the MNG has been dropped from consideration for the EPL as a consequence of its status as a non-commercial product. Evaluation is continuing as a part of a specific system.

The Multi Net Gateway's strengths are in its use of very strong methods of enforcing confidentiality, both cryptographically and by COMPUSEC design. The MNG protects user data and authenticates exchanges during intergateway communication by the distribution and use of cryptographic keys. The attribute that may most strongly recommend the FACC MNG for the basis of a TGG development is its certified kernel operating system.

The MNG does not, however, provide all the specific functions required by the TGG. Access control via TCP header port numbers and IP address pairs has been implemented under another DCA program and would need to be restructured in the TGG. Labeling of data traveling from between networks is not supported and would need to be added. The MNG's cost and performance are also disadvantages. The current unit cost of the MNG is on the order of $100,000, which may render it infeasible for the TGG. Higher performance levels than the 50 - 150 datagrams per second provided by the MNG could be obtainable for the TGG with advanced hardware, despite the additional processing required for labeling and access control.

5.1.2 The BBN Butterfly Gateway

The Butterfly Gateway has been under development and in use by Bolt, Beranek and Newman, Inc. since 1984. It is based upon the Butterfly general purpose parallel computing architecture consisting of multiple Motorola 680X0 processors (up to 256, each with memory and peripheral controllers) linked via an advanced interconnection network. The interconnection

network furnishes memory access pathways among all Motorola 680X0 processor components, so that any processor can potentially address any memory location. The Butterfly computer architecture has not been limited to communication applications but has also been applied to real time voice, scientific and artificial intelligence computing[14].

The Butterfly is a high performance gateway. The parallel architecture, widely accessible memory, and proliferated network controllers (per 680X0 processor system) can all provide increased datagram processing bandwidth. Multiple pathways between the network interfaces and the primary memory are provided by its architecture. The Butterfly operating system efficiently allocates tasks to process datagrams and to perform other gateway functions among the parallel processors. BBN has reported the processing rate using 16 CPUs as approximately 3000 datagrams per second. Butterfly gateways have been employed as core gateways in the DDN.

The Butterfly could serve as a suitable but not necessarily ideal transition vehicle for the TGG. Because it has a general purpose, albeit highly parallel, computer architecture, the features identified in Section 4 could incorporated in the Butterfly architecture via standard software developme processes. The strength of the BBN Butterfly gateway is its parallel architecture that provides high performance. However, the certification of parallel architectures represents significant challenges. The mapping of current COMPUSEC concepts onto a parallel processor architecture will be complex. This is a definite disadvantage in consideration of the Butterfly as a candidate TGG. Though the Butterfly could serve as a very high volume gateway, certification would pose a very significant technical risk.

5.1.3 Other Commercial Gateways

The proliferation of local area networks (LANs) to interconnect a number of machines in buildings and military bases has resulted in the development of gateway products by commercial vendors. Typically, such commercial gateway products interconnect Ethernets or IEEE 802 LANs with X.25 networks. These gateways particularly provide support for the DDN

---

14 IEEE Computer Architecture Technical Committee Newsletter, September/December, 1985. Contains set of technical papers on the Butterfly (TM) architecture and related applications.

Commercial gateway vendors include Proteon, Communication Machinery Corporation, Bridge Communications, CISCO, Unisys and ACC[15] [16].

Commercial gateways are based upon the current generation of 32-bit microprocessors, especially the Motorola 68020 and Intel 80386. A single central processor performs the protocol functions, while specialized processors, such as 8- and 16-bit microprocessors (e.g., the Intel 80286), provide services for the network interface. The overall throughput is limited by the rate at which the CPU can process datagrams and to a lesser extent by the rate at which the CPU can move data between primary memory and the network interface processors.

Commercial gateways are a suitable basis for future development of TGGs. The utility of 32-bit microprocessors for economical gateway implementations has been proven many times over, both with respect to hardware performance and with respect to ease of development via compilers, cross-compilers and development environments. Therefore, the features of both standard IP gateways and TGGs can be implemented via standard software development processes. The ultimate suitability of a particular commercial gateway model as a TGG vehicle will depend upon the soundness of the software design, the willingness of the vendor to work with the government toward certification goals, and the throughput that a single TGG must provide.

Figure 5.1.3-1 describes a set of features that distinguishes the six commercial gateways surveyed. All gateways are essentially identical in their use of IP between network interfaces.

---

15 SPARTA gratefully acknowledges information supplied by CISCO, CMC, Bridge, Proteon, Unisys and SRI, in response to requests.

16 Proceedings of the 2nd Annual TCP/IP Interoperability Conference, Alexandria, VA, December, 1987.

GATEWAY FEATURES					
VENDOR, PRODUCT	ROUTING PROTOCOLS	INTERFACES	DATAGRAMS/ SEC	NETWORK MANAGEMENT PROTOCOLS	ACCESS CONTROL
CISCO AGS-1E1D	RIP, HELLO	T1, V35, RS232 IEEE 802.3, X.25	220	CUSTOM TECHNIQUES; VENDOR IS WORKING IN IETF TO DEFINE STANDARDS;	YES; BASED ON IP ADDRESSES;
CMC DRN-3200	EGP, RIP SOON	RS232, V35, IEEE 802.3, X.25	242	CUSTOM TECHNIQUES; VENDOR IS WORKING IN IETF TO DEFINE STANDARDS;	YES; BASED ON IP ADDRESSES;
BRIDGE GB/1-IP	RIP NOW, EGP SOON	RS232, 422, V35, T1, X.25	2445	CUSTOM TECHNIQUES; VENDOR WILL CONSIDER USING IETF STANDARDS;	NO
ACC	NON NOW; REACHABILITY SOON;	T1, ISDN	100's	CUSTOM TECHNIQUES; VENDOR IS CONSIDERING ISO, IETF TECHNIQUES;	NOT DETERMINED;
PROTEON p4200	RIP, EGP, INTERIOR GATEWAY PROTOCOL	RS232, 422, V35 IEEE 802.3, X.25 SOON;	200	SGMP (RFC 1028); WILL ADHERE TO STANDARD WHEN DEFINED;	YES; HOST-DESTINATION ADDRESS PAIR BASED;
UNISYS MD386 DDN GATEWAY	EGP, INTERIOR GATEWAY PROTOCOL	IEEE 802.3, DDN X.25 DDN 1822, HDH	AS MANY AS DDN INTERFACE WILL ALLOW;	INFORMATION NOT AVAILABLE	INFORMATION NOT AVAILABLE

0488/028-008

FIGURE 5.1.3-1 GATEWAY FEATURES

The readiness of commercial gateway products for service as TGGs can be assessed from the table above. It is clear that most meet some primary TGG requirements:

- All products support elementary routing information exchange protocols and perform datagram routing.
- All products for which literature was received support X.25 or DDN network interfaces.
- All products can process packets quickly enough to fully utilize a bandwidth of 56,000 bits per second.

None of the commercial gateway products meet the functional requirements identified for TGGs in Section 4.5. Only the Proteon p4200 gateway currently meets a standard for network management. However, all vendors have expressed their interest in standards development. The problem in this area is that there are several candidate management standards (e.g., SGMP[17] and HEMS[18]). The need to decide among the candidates for use in the DDN may delay the standard's incorporation into applicable products.

One feature area that does differentiate these gateway products is their current access control capabilities. The Cisco, CMC and Proteon products are

---

17 SGMP, Simple Gateway Monitoring Protocol reference: RFC 1028

18 High Level Entity Management Standard references: RFC 1021-1024.

all capable of access control on an IP address basis. However, the current access controls do not meet TGG requirements as described in Section 4.5.

5.2 *Gateway Issues*

There is clearly a successful current generation of hardware architectures and software systems upon which gateway implementations can run, as made evident by current products. Nevertheless, the current internetworking approach is known to have problems and work continues on their solutions. Two major issues discussed in the internetworking community are congestion control and network management.

5.2.1 Internetwork Congestion Control and Gateway Performance

There are increasing concerns about limited gateway performance and resulting congestion. IP gateways are stateless by design and are consequently not capable of very effective responses to congestion[19]. On the other hand, the potential for congestion is increasing because of the bandwidth disparities between LANs and long haul nets and the increased use of LANs across DoD[20]. As the bandwidth available from LANs climbs through the 10s of Megabits per second range, the underlying bandwidth available to gateway CPUs is approached. Thus, traffic offered to a gateway by a LAN can easily swamp the gateway buffers. Currently, congestion of access lines is a problem. When access line bandwidth is expanded (e.g., by the use of T1 access lines with a rate of 1.544 megabits per second), gateway congestion is more likely to arise.

Remedies for this situation are the subject of current activities in the Internet Research and Development communities and include:

1) fairer and more effective mechanisms of throttling the traffic offered to gateways,

2) adding more gateways to the internet combined with effective routing algorithms to achieve traffic load leveling, and

3) increasing gateway throughput (as in the case of the Butterfly gateways) as available bandwidth grows.

Compared to the pace of growth of the bandwidth available from LANs, the remedies will be slower in maturing. Already, the bandwidth available

---

19 Zhang, L., "Designing a New Architecture for Packet Switching Communication Networks," IEEE Communications Magazine-Vol. 25. No. 9 (Sept. 1987), pp. 5-12.

20 DDN Premises Technology Study, BBN, 1986.

through local interconnection media, such as FDDI[21] approaches the bandwidth available internally to gateway CPUs. Because there is a considerable amount invested in the current Internet software architecture, the first two remedies presented above must first be investigated and later approved by consensus. The third remedy above also requires time to develop, due to the pace in corresponding development of parallel and high-speed computing architectures.

Very significant increases in gateway speed may be possible using special purpose architectures, perhaps coupled with simplified protocol processing requirements. For example, Xilinx[22] describes the synthesis of a processor for handling T1 data based upon their programmable gate array. T1 data formats are fixed and strongly positional so that hardware processing means can be used to locate control bits and perform control functions. To date, however, gateways have been implemented using general purpose rather than special purpose CPUs. None of the current gateway vendors has plans for extremely high performance architectures, even though they all realize that gateway bandwidth is already a limiting factor in access to wide area networking.

5.2.2 TGG Software Prospects

Gateway software is readily available, as made evident by the variety of gateway products and by the more than 160 gateways registered in the DoD Internet. Gateway software includes IP protocol processing including routing decisions as necessary, generation of and response to ICMP[23] messages, operation of network interfaces, exchange of gateway to gateway messages by EGP or other gateway to gateway protocols, and the exchange of network management and related user support messages. So long as the requirements for these functions remain stable, gateway software can be competitively priced.

Concerns with the Internet architecture, especially at the level of IP gateways, may drive new requirements for gateway software. For example, IP protocol processing may change to require gateways to maintain state information, including tracking flows between sources and destinations. Potential changes of this type may contribute to gateway software expense in the near future, but the schedule and direction of such changes are presently uncertain. Detailed standard specifications of network and internetwork

---

21 IEEE 802.6, Fiber-Optic Digital Data Interface

22 The Programmable Gate Array Design Handbook First Edition, (Xilinx, Inc., San Jose, CA, 1986), pp. 3-45 - 3-53, "A T1 Communications Interface".

23 RFC 792, Internetwork Control Management Protocol

management paradigms are now under consideration. Even though resulting capabilities will be advanced, the standardization of management features will limit both developers' and users' costs for them.

The additional TGG security features described in Section 4 do constitute a significant set of additional requirements. Their complexity and code volume would comprise a noticeable fraction (10% - 25%) of an overall standard IP gateway implementation. However, the development cost of the security features will be affected more by the certification requirements than by size and complexity. Consequently, the purely developmental costs for a TGG could be very reasonable, but the overall TGG acquisition cost will certainly be increased by the need to certify portions of the software, including the operating system kernel and the security mechanisms (i.e., labeling and access control).

Experience with software certification has been limited. Five general purpose operating systems have been certified at levels from C2 to A1; three add-on packages have been certified at the C1 or C2 levels. Also, certification has been a lengthy process, requiring significant effort on the part of the both government and the developer. Certification requirements, as stated in the NCSC Orange Book and TNI go well beyond commercial standards for software quality assurance. On the order of 10 staff years may be required to certify an operating system kernel and selected security mechanisms as required by the TGG. Consequently, development costs attributable to certification could be on the order of $1,000,000.

As an insight into the certification process for the TGG, the following list represents security-relevant requirements which would be the focus of a certification process.

- the gateway always labels data going from low side to high side network(s);
- labels attached to networks are always accurate;
- the gateway always performs access control at IP levels in accordance with access control host pair lists, masks, formulas, etc.
- the gateway provides audit trails for initialization and modifications of access control host pair data;
- the gateway always performs access control at transport protocol levels in accordance with access control port (transport protocol connection identifier) lists, masks, formulas, etc.; and
- the gateway provides audit trails for initialization and modifications of access control port data.

These requirements support the TGG security properties of providing data labels for and providing discretionary access control to its network(s).

5.3 Conclusion

Hardware and software technologies are currently available for direct application to the development of a TGG. Acquisition possibilities are not limited by any known technology hurdles. Only the growing use of high bandwidth local area networking to provide access for multiple hosts into the wide area DDN (with less bandwidth to be shared among more hosts) presents a technology problem. However, this problem area is not limited to TGG applications, but covers gateway applications in general.

A major hurdle in the overall acquisition and implementation process is the certification of the TGG software and hardware. This process will be a major expense, given the number of requirements, the thoroughness with which they must be addressed, and the relative shortage of experience with the certification process.

This outlook suggests that attention should be given to existing work and accomplishments in the development of trusted computing bases (TCB). These are exemplified by SCOMP, Multics and UTX (Gould's Unix-like operating system.) Additional work on secure Unix is underway as well. These TCBs are operating system kernels certified to provide a range of security functions within a multi-processing environment. Versions of secure Unix and Unix-like operating systems could be bases from which TGG development economies could be gained, especially since Unix has been used previously as a base for packet switching systems (e.g., DTI's Network Front End). The specific functions for the TGG could be developed within the Unix-like environment, using the furnished calls to provide all accesses of subjects (processes) to objects. Although additional certification would be require beyond the kernel, the overall certification effort would be greatly simplifi by the use of a certified kernel operating system. This implementation strategy will be examined in detail in the second phase of this effort.

There is a clear advantage to basing the TGG, as much as possible, on off-the-shelf technology and products. Both initial acquisition and subsequent logistics support can experience significant dollar savings. The review of gateway technology leads to the conclusion that additions to off-the-shelf hardware and software technology could be sufficient for a TGG.

6.0 TGG Quantity Estimate

This section presents an analysis of the estimated number of TGGs required for the DDN. Section 6.1 concentrates on the TGGs required to support the MILNET/DISNET interface. Sections 6.2 and 6.3 postulate numbers of TGGs required for the ARPANET/MILNET and Closed/Open Community interfaces respectively.

6.1 MILNET/DISNET TGGs

To determine the number of TGGs necessary to adequately service MILNET/DISNET requirements, several systems were examined. They were surveyed to discover their applications and missions, and the nature of their interest or non-interest in TGG services. Based upon interviews with these points of contact, a projection of TGG requirements for the DDN as a whole was developed. The estimates rely on the assumption that the interview data is a representative sampling of future DDN systems and applications. The sample is characterized by a percentage of systems with a requirement or interest in cross-segment connectivity as exemplified by MIS-style applications and a percentage of systems without such an interest as exemplified by automated surveillance systems.

A simple calculation was used to estimate the number of TGGs to support planned and anticipated user requirements in the 1990s. The assumptions used in the calculation are described below.

Assumption 1. The capacity of a single TGG is estimated at 200 datagrams per second, each carrying 1000 bits of data.

The processing rate is based upon a survey of the throughputs obtained from commercial single processor gateways. As shown in Table 5-1, the processing rate for single processor gateways ranges from 100-250 datagrams per second for 1000 bit datagrams. By obtaining an estimate of the number of instructions necessary to process a datagram (about 500 instructions per datagram), the amount of required overhead for the addition of required security services can be calculated. This calculation indicates that the performance range would only be slightly lowered to 80-220 datagrams per second. Further calculations use a high average of 200 datagrams per second per gateway.

Assumption 2. The number of hosts expected to use a TGG for our sample (Appendix A) was estimated by weighting system's host counts in accordance with the category: 100% for "A"; 50% for "B" and "C"; and 0% for "D". These weights aim to avoid possible bias in counting the hosts.

Assumption 3. The intersegment DDN bandwidth requirement is estimated at 760 - 1150 datagrams per second, so that a single TGG could support on the order of 35 - 50 host machines.

The bandwidth requirement is based on a survey of systems placed in the "A" category, indicating relatively large systems with well defined requirements expressing a definite need for a TGG. A total of 14 systems were contacted again for this purpose. Five of these contacts resulted in useful information: CABIN, FNOC-NEDN, ARFCOS, MAC C2 IPS and CLAM.

For the most part, these five contacts were either unable to specify or were sensitive about specifying the kinds, amount, and frequency of data that they might need to access or send through the TGG. However, information about the general kinds of data to be used, as well as current quantity and frequency estimates, were obtained.

The results indicate that contacts could be grouped into two kinds of applications: those with low data rate requirements and those with high data rate requirements. The low data rate group includes those systems using the TGG to send small files only on an infrequent basis (e.g. daily). Systems with a need for database access or updates also fall into this category. It is not likely that these types of systems will drive the number of required TGGs. The high data rate group, those who need to send large files frequently, will be more likely to determine the number of TGGs necessary. In order to calculate the overall application bandwidth, both the transfer rate per host and the number of hosts in this group must be estimated. By estimating the average transfer rate for file transfer applications (FTP) as 4 - 6 datagrams per second per host and the percentage of hosts in the high data rate group to be 30% based on those systems contacted, the overall application bandwidth can be calculated as illustrated in Figure 6.1-1. This assumption also relies on the segments being capable of supporting the associated host data rates.

It should be noted that the level of confidence in this figure is moderate due to the sample size, the level of information obtained, and the estimation necessary for the FTP transfer rate and the percentage of high data rate systems. Substantial increases in either of these estimations will result in an increase in the number of TGGs. An adjustment factor of 2 was used in the final calculations to compensate for low numbers in two areas: (1) the systems contacted specified that no electronic mail messages would be necessary, however it is anticipated that this may change when the TGG is operational, and (2) there is expected to be a significant increase in the number of systems requiring high data rates.

Assumption 4. Estimates are based on aggregate host counts and do not consider advantages of optimal geographic location.

As the survey proceeded, it became apparent that topology could be an important factor in accurately estimating the number of TGGs required. While a small amount of information was gathered through the URDB, this is an area that might well profit from deeper investigation in the future. For this report, it is assumed that every N hosts, accounted for by our weighted method, will require a TGG.

Based upon these assumptions and the projection of the sample present-day requirement statistics projected onto the full URDB system and host projections, 120 DISNET systems will be operating, using services of approximately 730 hosts.[24] Therefore, as shown in Figure 6.1-1, 9 - 12 TGGs are estimated to be required to meet Internetworking requirements between the MILNET and the DISNET.

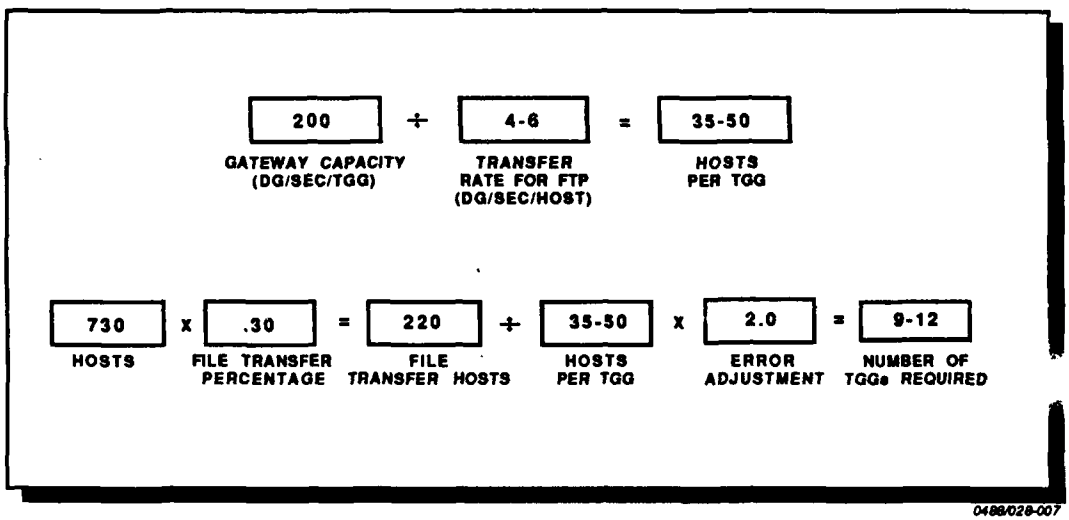


FIGURE 6.1-1 ESTIMATION OF QUANTITIES OF REQUIRED TGGs

6.2 ARPANET/MILNET TGGs

The ARPANET and MILNET are connected today by both mailbridges, which operate today as full service IP gateways, and through a number of back channels. The seven mailbridges are handling on the order of 1,000,000 datagrams each per day. At this level, these gateways are heavily congested. Based on an analysis of the ARPANET/MILNET traffic performed in December of 1986[25], approximately 60% of the traffic would be permitted, given proposed TGG rules (SMTP and MILNET initiated FTP). A more

---

24 We found 26 systems whose category-weighted host count was 158.

25 Report on Mailbridge Traffic by TCP Port, BBN, December 1986

complete breakdown by percentage of this traffic study is depicted in Figure 6.2-1. In order for the TGGs to effectively enforce access control, back channel connections must be eliminated. The traffic from these paths would then pass through TGGs. While it is difficult to estimate the volume of this traffic, we will assume that it will approximately balance the reductions gained from the access control rules. This implies an ARPANET/MILNET traffic load of about current levels and consequently, based on the current congested status, a number of ARPANET/MILNET TGGs in the range of 8 - 10.

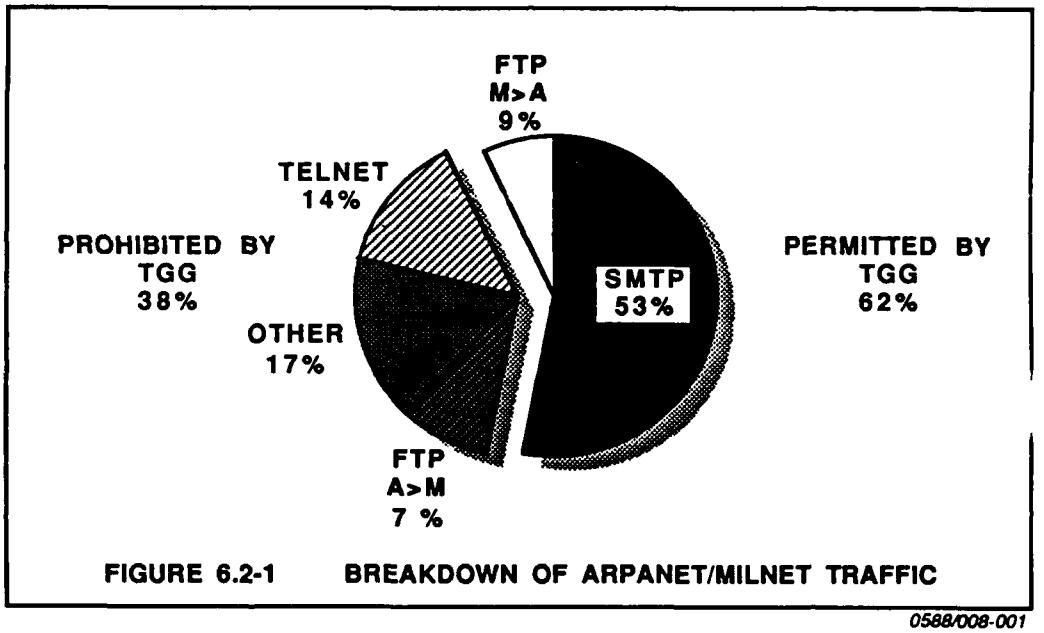


FIGURE 6.2-1 BREAKDOWN OF ARPANET/MILNET TRAFFIC

0588/008-001

6.3 Closed/Open Community TGGs

A similar set of calculations could be applied to Closed/Open community requirements. However, data leading to such a calculation is currently unavailable. There are no current examples for analyzing Closed and Open communities based upon certification status, because DDN users have not yet formulated their certification plans. While no estimates are available for any interconnection requirements or volumes, if the Closed/Open Community TGG is used to support transitions and is deployed on a per community basis the number of TGGs should be in 5-10 range.

ACKNOWLEDGEMENTS

Mike Corrigan, OSD

Julian Gitlin, WIS JPMO

Carl Landwehr, NRL

Brad Harnish, RADC

Pat Sullivan, DCEC

Len Tobacchi, DDN PMO

Lt. Col. Russ Mundy, DDN PMO

Dick Hale, DCEC

Sherrill Adkins, DCEC

Lt. Col. Larry Hill, DCA PAC

Royce Harrison, DDN PMO

Bill Randall, DCA EUR

Jim Steinmeyer, NSA

Sue Reissig, Mitre

Dave Gomberg, Mitre

Ed Knepley, DCEC

Marty Fisher, DCEC

Bill Hale, DCEC

Zaw Sing Su, SRI

Carl Sunshine, Unisys

And a special thanks to those folks at DCEC for their timely and friendly help with the URDB:

L. E. Conway

Lt. Joe Alino

Jackie Hubbard

APPENDIX

SYSTEM ACRONYM: AC2SMAN1

FULL SYSTEM NAME: Alaskan Air Command, Command and Control System Military Automated Network -1

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 10/30/88

SYSTEM ACRONYM: AFEWS

FULL SYSTEM NAME: Air Force Electronic Warfare System

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: AFHRC

FULL SYSTEM NAME: Air Force Historical Research Center

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: AFSAC

FULL SYSTEM NAME: Air Force Special Activities Center

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET
CLASSIFICATION: SECRET
INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: AMPMOD

FULL SYSTEM NAME: Army Material Plan Modernization
AGENCY: ARMY
NETWORK ASSIGNMENT: DISNET
CLASSIFICATION LEVEL: SECRET
INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: ARFCOS

FULL SYSTEM NAME: Armed Forces Courier Service
AGENCY: JOINT CHIEFS OF STAFF
NETWORK ASSIGNMENT: DISNET
CLASSIFICATION LEVEL: SECRET
INIT. OPER. CAP. DATE: 01/01/88

SYSTEM ACRONYM: BSMS

FULL SYSTEM NAME: Battle Staff Management System
AGENCY: AIR FORCE
NETWORK ASSIGNMENT: DISNET
CLASSIFICATION LEVEL: SECRET
INIT. OPER. CAP. DATE: 01/01/90

SYSTEM ACRONYM: CABIN

FULL SYSTEM NAME: Command Automated Budget Info Net

AGENCY: AIR FORCE

NETWORK ASSIGNMENT

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 06/22/87

SYSTEM ACRONYM: CAIMS

FULL SYSTEM NAME: Conventional Ammunition Integrated Manageme

AGENCY: NAVY

NETWORK ASSIGNMENT: MILNET[26]

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: CLAM

FULL SYSTEM NAME: Computer Link AFTAC McClellan

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

---

26 This assignment was originally indicated as DISNET in the URDB. Classification was not changed when the new information was entered.

SYSTEM ACRONYM: CCS-C; CCS-U

FULL SYSTEM NAME Central Computer System - Classified; Central Computer System - Unclassified

AGENCY: NAVY

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: CCSA-NET

FULL SYSTEM NAME: Conus Communications Support Agency

AGENCY: ARMY

NETWORK ASSIGNMENT: WINCS

CLASSIFICATION LEVEL: TOP SECRET

INIT. OPER. CAP. DATE: 12/15/88

SYSTEM ACRONYM: COMINEWARCOM

FULL SYSTEM NAME: Commander Mine Warfare Command

AGENCY: NAVY

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 06/30/88

SYSTEM ACRONYM: DCA-WWOLS

FULL SYSTEM NAME: DCA World Wide On-Line System

AGENCY: DCA

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: DMA-SMTP

FULL SYSTEM NAME: Defense Mapping Agency - Special Mission Tracking Program

AGENCY: DMA

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: DMA-S&T

FULL SYSTEM NAME: DMA Scientific and Technology

AGENCY: DMA

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: DROLS

FULL SYSTEM NAME: Defense Research & Development On-Line System

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 06/01/88

SYSTEM ACRONYM: EWIR-NIS

FULL SYSTEM NAME: Electronic Warfare Integrated Reprogramming-Network Interface System

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 06/01/88

SYSTEM ACRONYM: FNOC-NEDN

FULL SYSTEM NAME: Fleet Numerical Oceanographic Center - Navy Environmental Data Network

AGENCY: NAVY

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 12/01/89

SYSTEM ACRONYM: GOAP

FULL SYSTEM NAME: Geostat Ocean Application Program

AGENCY: NAVY

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 06/30/88

SYSTEM ACRONYM: IAIPS

FULL SYSTEM NAME: Integrated Automated Intelligence Processing System

AGENCY: NAVY

NETWORK ASSIGNMENT: SCINET

CLASSIFICATION LEVEL: TOP SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

SYSTEM ACRONYM: MAC C2 IPS

FULL SYSTEM NAME: MILITARY AIRCRAFT AND COMMAND, COMMAND AND CONTROL INFORMATION PROCESSING SYSTEM

AGENCY: AF

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 08/01/89

SYSTEM ACRONYM: JSS

FULL SYSTEM NAME: Joint Surveillance System

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 01/01/90

SYSTEM ACRONYM: SDI

FULL SYSTEM NAME: Strategic Defense Initiative

AGENCY: OSD

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 12/31/87

SYSTEM ACRONYM: SSN

FULL SYSTEM NAME: Space Surveillance Network

AGENCY: AIR FORCE

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: 04/01/90

SYSTEM ACRONYM: TRINET

FULL SYSTEM NAME: Trident Logistics Data System Network

AGENCY: CIVILIAN NAVY

NETWORK ASSIGNMENT: DISNET

CLASSIFICATION LEVEL: SECRET

INIT. OPER. CAP. DATE: NOT AVAILABLE

TABLE A-1 SURVEYED SYSTEMS AND POINTS OF CONTACTS - CATEGORY A

SYSTEM	HOSTS, TERMS	CONTACT	AGENCY	CLASS
AC2SMAN1: ALASKAN AIR COMMAND, COMMAND AND CONTROL SYSTEM MILITARY AUTOMATED NETWORK	1,3	*CPT SIEVERT (MSGT GRAY)	AF	S
ARFCOS: ARMED FORCES COURIER SERVICE	37,0	R. COONEY	JCS	S
CABIN: COMMAND AUTOMATED BUDGET INFORMATION NETWORK	2,0	*B. ATKINSON (N. BASFORD)	AF	S
CLAM: COMPUTER LINK AFTAC MCCLELLAN	10,0	CPT MASSEY	AF	S
CCS-C & U: CENTRAL COMPUTER SYSTEMS - CLASSIFIED & UNCLASSIFIED	9,0	W. WILLIAMS	NAVY	S
COMINEWAR-COM: COMMANDER MINE WARFARE COMMAND	2,0	D. ROACH	ARMY	S
DCA-WWOLS: DCA WORLD-WIDE ON-LINE SYSTEM	1,0	*CPT GUSUKUMA (LTC) TITTLE	DCA	S
FNOC-NEDN: FLEET NUMERICAL OCEANOGRAPNIC CENTER - NAVY ENVIRONMENTAL DATA NETWORK	22,0	M. PETERSON	AF	S
SDI: STRATEGIC DEFENSE INITIATIVE	6,0	CDR MOORE	OSD	S
TRINET: TRIDENT LOGISTICS DATA SYSTEM	7,8	R. DASILVA	NAVY	S
MAC C2 TPS: MILITARY AIRCRAFT AND COMMAND, COMMAND AND CONTROL INFORMATION PROCESSING SYSTEM	40,0	LT SIEBOLD	AF	S

0488/029-007

( ) INITIAL CONTACT
* NEW CONTACT

TABLE A-2 SURVEYED SYSTEMS AND POINTS OF CONTACT - CATEGORY B

SYSTEM	HOSTS, TERMS	CONTACT	AGENCY	CLASS
AFHRC: AIR FORCE HISTORICAL RESEARCH CENTER	1,250	T. DEAN	AF	S
BSMS: BATTLE STAFF MANAGEMENT SYSTEM	8,0	LTC CATO	AF	S
CAIMS: CONVENTIONAL AMMUNITION INTEGRATED MANAGEMENT SYSTEM	1,56	L. MATTHEWS	NAVY	S
DMA-SMTP: DEFENSE MAPPING AGENCY SPECIAL MISSION TRACKING PROGRAM	1,50	J. NICHOLS	DMA	S

0488/029-007A

( ) INITIAL CONTACT
* NEW CONTACT

TABLE A-3 SURVEYED SYSTEMS AND POINTS OF CONTACT - CATEGORY C

SYSTEM	HOSTS, TERMS	CONTACT	AGENCY	CLASS
AFSAC: AIR FORCE SPECIAL ACTIVITIES CENTER	2,0	*CPT HILLSMEN (CPT SMITH)	AF	S,SCI
AMP-MOD: ARMY MATERIAL PLAN MODERNIZATION	1,56	P. TRALL	ARMY	S
DMA-S&T: DEFENSE MAPPING AGENCY SCIENTIFIC AND TECHNOLOGY	2,0	D. KINDSFATHER	DMA	S
DROLS: DEFENSE RESEARCH AND DEVELOPMENT ON-LINE SYSTEM	1,0	M. BRZEZINSKI	DS	S
IAIPS: INTEGRATED AUTOMATED INTELLIGENCE PROCESSING SYSTEM	10,0	CDR MCDOUGALL	AF	TS/SCI

0488/029-007B

( ) INITIAL CONTACT
* NEW CONTACT

TABLE A-4 SURVEYED SYSTEMS AND POINTS OF CONTACT - CATEGORY D

SYSTEM	HOSTS, TERMS	CONTACT	AGENCY	CLASS
AFEWS: AIR FORCE ELECTRONIC WARFARE SYSTEM	15,0	H. B. JENNINGS	AF	S
CCSA-NET: CONUS COMMUNICATION SUPPORT AGENCY NETWORK	9,0	J. SARIANO	ARMY	S
EWIR-NIS: ELECTRONIC WARFARE INTEGRATED REPROGRAMMING NETWORK INTERFACE SYSTEM	105,0	E. WILLIAMS	AF	S
GOAP: GEOSTAT OCEAN APPLICATION PROGRAM	3,0	P. MOERSDORF	NAVY	S
JSS: JOINT SURVEILLANCE SYSTEM	6,0	CPT LANGHALS	AF	S
SSN: SPACE SURVEILLANCE NETWORK	14,1	CDR LANGHALS	AF	S

( ) INITIAL CONTACT
* NEW CONTACT

0488/029-007C